Two-Round and Non-Interactive Concurrent Non-Malleable Commitments from Time-Lock Puzzles*

Huijia Lin† Rafael Pass‡ Pratik Soni§

Abstract

Non-malleable commitments are a fundamental cryptographic tool for preventing (concurrent) man-in-the-middle attacks. Since their invention by Dolev, Dwork, and Naor in 1991, the round-complexity of non-malleable commitments has been extensively studied, leading up to constant-round concurrent non-malleable commitments based only on one-way functions, and even 3-round concurrent non-malleable commitments based on subexponential one-way functions, or standard polynomial-time hardness assumptions, such as, DDH and ZAPs.

But constructions of *two-round*, or *non-interactive*, non-malleable commitments have so far remained elusive; the only known construction relied on a strong and non-falsifiable assumption with a non-malleability flavor. Additionally, a recent result by Pass shows the impossibility of basing two-round non-malleable commitments on falsifiable assumptions using a polynomial-time black-box security reduction.

In this work, we show how to overcome this impossibility, using super-polynomial-time hardness assumptions. Our main result demonstrates the existence of a two-round concurrent non-malleable commitment based on sub-exponential "standard-type" assumptions—notably, assuming the existence of all four of the following primitives (all with subexponential security): (1) non-interactive commitments, (2) ZAPs (i.e., 2-round witness indistinguishable proofs), (3) collision-resistant hash functions, and (4) a "weak" time-lock puzzle.

Primitives (1),(2),(3) can be based on e.g., the discrete log assumption and the RSA assumption. Time-lock puzzles—puzzles that can be solved by "brute-force" in time 2^t, but cannot be solved significantly faster even using parallel computers—were proposed by Rivest, Shamir, and Wagner in 1996, and have been quite extensively studied since; the most popular instantiation relies on the assumption that 2^t repeated squarings mod $N = pq$ require "roughly" 2^t parallel time. Our notion of a "weak" time-lock puzzle requires only that the puzzle cannot be solved in parallel time 2^{t^ε} (and thus we only need to rely on the relatively mild assumption that there are no *huge* improvements in the parallel complexity of repeated squaring algorithms).

We additionally show that if replacing assumption (2) for a non-interactive witness indistinguishable proof (NIWI), and (3) for a *uniform* collision-resistant hash function, then a *non-interactive* (i.e., one-message) version of our protocol satisfies concurrent non-malleability w.r.t. uniform attackers. Finally, we show that our two-round (and non-interactive) non-malleable commitments, in fact, satisfy an even stronger notion of Chosen Commitment Attack (CCA) security (w.r.t. uniform attackers).

*A prelimiary version of this submission appeared at FOCS 2017.

†Paul G. Allen School of Computer Science and Engineering, University of Washington, Seattle, WA, 98195 rachel@cs.washington.edu.

‡Department of Computer Science, Cornell NYC Tech, New York City, NY, 10044 rafael@cs.cornell.edu.

§Department of Computer Science, University of California Santa Barbara, Santa Barbara, CA, 93106 pratik_soni@cs.ucsb.edu.

Contents

1 Introduction **1**
- 1.1 Our Results . . . 2
- 1.2 Concurrent and Independent Work . . . 5
- 1.3 A Perspective: Non-Malleability from Hardness in Different Axes . . . 6
- 1.4 Organization . . . 6

2 Overview **6**
- 2.1 Towards Overcoming the Impossibility Result . . . 8
- 2.2 Full-Fledged Non-Malleable Commitments . . . 11
- 2.3 Extensions . . . 13

3 Preliminaries **14**
- 3.1 Basic Notation . . . 14
- 3.2 Circuit Classes . . . 15
- 3.3 Indistinguishability and One-wayness . . . 15
- 3.4 Witness Relation, ZAP and NIWI . . . 17
- 3.5 Commitment Schemes . . . 18
- 3.6 Time-Lock Puzzles . . . 22
- 3.7 Collision-resistant Hash Functions . . . 24

4 Basic Commitment Schemes **24**
- 4.1 Depth-robust Over-extractable Commitment Scheme from a TL-puzzle . . . 24
- 4.2 Size-robust Over-extractable Commitment Scheme from Injective OWFs . . . 26
- 4.3 Strong Over-extractable Commitment Scheme . . . 28

5 Non-malleable Commitment Scheme w.r.t. Extraction for Short Identities **30**

6 Strengthening Non-malleability **33**
- 6.1 A Bare-Bone Protocol and Challenges . . . 33
- 6.2 Building Blocks . . . 35
- 6.3 Commitment Scheme $\langle \widehat{C}, \widehat{R} \rangle$ . . . 36
- 6.4 Proofs of Claims from Section 6.3 . . . 44

7 Amplifying Length of Identities – Log n trick **56**

8 Concurrent Non-malleable Commitment for n-bit Identities **60**
- 8.1 Commitment Scheme $\langle C^*, R^* \rangle$ . . . 60
- 8.2 Instantiations . . . 61
- 8.3 Efficiency of $\langle C^*, R^* \rangle$ . . . 66
- 8.4 Security of $\langle C^*, R^* \rangle$ . . . 69

9 Two-round Robust CCA-secure Commitment **70**
- 9.1 CCA-secure Commitment w.r.t. Committed-Value Oracle . . . 71
- 9.2 k-Robustness w.r.t. Committed-value Oracle . . . 72
- 9.3 Proof of Robust CCA-security of $\langle \widehat{C}, \widehat{R} \rangle$ . . . 72
  - 9.3.1 Proof of CCA-security . . . 73
  - 9.3.2 Proof of Robustness . . . 77

10 Non-interactive Concurrent Non-Malleable and CCA-secure Commitment against Uniform Adversaries **78**
10.1 Non-malleability against Uniform Adversaries 79
10.2 Robust CCA-security against Uniform Adversaries 79
10.3 1-Message Security Strengthening Technique 80

11 Appendix **85**
11.1 Proof of Theorem 15 85

1 Introduction

Commitment schemes are one of the most fundamental cryptographic building blocks. Often described as the "digital" analogue of sealed envelopes, commitment schemes enable a *sender* to commit itself to a value while keeping it secret from the *receiver*. This property is called *hiding*. Furthermore, the commitment is *binding*, and thus in a later stage when the commitment is opened, it is guaranteed that the "opening" can yield only a single value determined in the committing stage.

For many applications, however, the most basic security guarantees of commitments are not sufficient. For instance, the basic definition of commitments does not rule out an attack where an adversary, upon seeing a commitment to a specific value v, is able to commit to a related value (say, $v-1$), even though it does not know the actual value of v. To address this concern, Dolev, Dwork and Naor (DDN) introduced the concept of *non-malleable commitments* [DDN00]. Loosely speaking, a commitment scheme is said to be non-malleable if it is infeasible for an adversary to "maul" a commitment to a value v into a commitment to a related value $\tilde{v}$. The notion of a *concurrent non-malleable commitment* [DDN00, PR05a] further requires non-malleability to hold even if the adversary receives many commitments and can itself produce many commitments.

The first non-malleable commitment protocol was constructed in the original work of [DDN00] in 1991, based on the minimal assumption of one-way functions. The first concurrently secure construction was provided by Pass and Rosen in 2005 [PR05a]. Since then, a central question in the study of non-malleability has been to determine the exact number of communication rounds needed for achieving (concurrent) non-malleable commitments. Significant progress has been made over the years [Bar02, PR05a, PR05b, LPV08, LP09, PPV08, PW10, Wee10, Goy11, LP11, GLOV12]. The current state-of-the-art is that 4-round concurrent non-malleable commitments can be constructed based on one-way functions [COSV17], 3-round concurrent non-malleable commitments can be constructed from subexponentially-secure one-way permutations [COSV16, GPR16], and very recently can be based only on the polynomial hardness of either DDH or Quadratic-residousity or N^{th}-residuosity and ZAPs [Khu17].

On the Existence of Two-Round or Non-Interactive Non-malleable Commitments. The situation changes drastically when it comes to two-round or non-interactive (i.e., one-message) protocols: Pandey, Pass and Vaikuntanathan [PPV08] provided a construction of a non-interactive non-malleable commitment based on a new *non-falsifiable* hardness assumption, namely, the existence of an *adaptively-secure injective one-way function*—roughly speaking, a one-way function f that is hard to invert on a random point $y = f(x)$ even if you get access to an inversion oracle that inverts it on every *other* point $y' \neq y$. This assumption is not falsifiable since the inversion oracle cannot be implemented in "real-life"[1]; additionally, note that the assumption also has a strong non-malleability flavor—in particular, the assumption would clearly be false if one could "maul" $y = f(x)$ to e.g., $y' = f(x+1)$. As such, a question that remains open is whether we can obtain two-round "non-malleability" from "pure scratch" (i.e., from "hardness" alone). Indeed, a recent work by Pass [Pas13] showed that there are some inherent limitations to reducing 2-round non-malleability to falsifiable assumptions. More precisely, Pass shows that if there exists a 2-round non-malleable commitment that can be proven secure using a polyomial-time (or even super-polynomial, but security preserving[2]) black-box reduction R to a falsifiable assumption, then

[1] More precisely, an assumption is falsifiable if it can be modeled as a game between an efficient challenger and an adversary. The adaptive security of injective one-way functions cannot be modeled in such a way as no efficient challenger can implement the inversion oracle in the game with the adversary.

[2] Here, by security preserving, it means that the security reduction uses an adversary breaking the security of the cryptographic scheme under analysis w.r.t. one security parameter n, to break the underlying hardness assumption

the reduction R can itself be used to break the assumption. In particular, this rules out basing 2-round non-malleability (using black-box reduction) on falsifiable hardness assumptions against polynomial time adversaries.

Towards overcoming this barrier, a recent work by Goyal, Khurana and Sahai [GKS16] presents a two-message protocol in a stronger "synchronous model" of communication (and achieving only a weaker notion of non-malleability "w.r.t. opening"). In this work, we focus on the standard communication model (and the standard notion of non-malleability) and explore whether super-polynomial-time hardness assumptions (and using non-security preserving reductions) can be used to overcome this barrier:

Can we construct non-interactive or 2-round non-malleable commitment from super-polynomial hardness assumptions?

1.1 Our Results

Our main result demonstrates the existence of a two-round concurrent non-malleable commitment scheme based on sub-exponential hardness assumptions—notably, assuming the existence of the following primitives (all with subexponential security): (1) non-interactive commitments, (2) ZAPs (i.e., 2-round witness indistinguishable proofs) [DN00], (3) collision-resistant hash functions, and (4) a "weak" time-lock puzzle [RSW96].

Primitives (1),(2),(3) are all very commonly used and can be based on e.g., the discrete log assumption and the RSA assumption. Primitive (4) deserves some more discussion: *Time-lock puzzles*—roughly speaking, puzzles that can be solved in "brute-force" in time 2^t, but cannot be solved "significantly faster" even using parallel computers—were proposed by Rivest, Shamir, and Wagner in 1996 [RSW96] (following May's work on timed-release cryptography [May93]), and have since been quite extensively used in the area of timed-release cryptography. A bit more precisely, a $(T(\cdot), B(\cdot))$-*time-lock puzzle* enables a "sender" to efficiently generate a puzzle puzz with a designated "level" of hardness $t = t(n)$ along with its unique solution s, where n is the security parameter, so that: (i) the puzzle solution can be found in (uniform) time 2^t, but (ii) the puzzle solution cannot be recovered by any attacker of size at most $B(n) > 2^t$ with (parallel) running-time (i.e., circuit depth) at most $T = T(t)$ (where $T(t) << 2^t$ determines the "hardness gap" of the puzzle).[3] Typical applications of time-lock puzzles only require security against polynomial-size attackers, thus it suffices to let $B(\cdot)$ be any slightly super-polynomial function; however, they require the hardness gap to be very small—namely, $T = 2^{\delta t}$ or even $T = \delta 2^t$ for some $\delta < 1$ (i.e., the problem is inherently "sequential" and the honest puzzle solver is essentially optimal, even if you have access to parallel computers). In this work, we will need security against subexponential-size attackers, but in contrast, only require the existence of a time-lock puzzle with a relatively "large" hardness gap—we only need the puzzle to be hard to break for time $T = 2^{t^\varepsilon}$ for some constant $0 < \varepsilon < 1$.

Theorem 1 (Main Theorem, Informal)**.** *Let T and B be two arbitrary subexponential functions. Assume the existence of non-interactive commitments, a ZAP, a family of collision-resistant hash functions, all with subexponential-security, and the existence of a (T, B)-time-lock puzzle. Then, there exists a 2-round concurrent non-malleable commitment.*

w.r.t. the same security parameter $n' = n$. On the other hand, if n' is different from, in particular smaller than n, the reduction is said to be non-security preserving.

[3] Time-lock puzzles as defined are falsifiable as the challenger can efficiently (in time $\mathsf{poly}(t, n) = \mathsf{poly}(n)$) sample a puzzle puzz together with its unique solution s.

The original construction of time-lock puzzles due to Rivest, Shamir, and Wagner [RSW96] is based on the hardness of a very natural strengthening of the factoring problem referred to as the *repeated squaring problem*: given a random RSA-modulus $N = pq$, and a random (or appropriately chosen) element g, compute

$$g^{2^{2^t}} \bmod N$$

Clearly, this can be done using 2^t repeated squarings. The RSW assumption is that this task cannot be significantly sped up, even using parallel resources, as long as the total resource of the adversary does not enable factoring N. Given the current state-of the art, the repeated squaring problem appears to be hard for *strongly exponential* parallel-time: $T(t) = \delta 2^t$ (that is, basically, no non-trivial speed-up over repeated squaring is possible); indeed, this strong assumption is typically used in the literature on timed-release cryptography (in fact, several significantly stronger versions of this assumption, where additional leakage is given, are also typically considered—see e.g., the "generalized Blum-Blum-Shub assumption" of Boneh-Naor [BN00].)

Since we only need a "weakly"-secure time-lock puzzle where the hardness gap is large, it suffices for us to make a significantly weaker, *subexponential*, repeated squaring assumption, that is,

$$2^t \textit{ repeated squarings (modulo } N = pq\textit{) cannot be done in parallel-time } 2^{t^\varepsilon}$$

More formally:

Assumption 1 (Subexp. Repeated Squaring Assumption, Informal)**.** *There exists subexponential functions T, B such that for every function $t(n) \in \omega(\log n) \cap n^{O(1)}$, the following holds: For every size $B(\cdot)$-attacker A with (parallel) running-time (i.e,. circuit depth) at most $T(t(\cdot)) < B(\cdot)$, there exists a negligible function μ such that for every $n \in \mathbb{N}$, the probability that A, given g, N where N is a randomly chosen n-bit RSA-modulus, and g is a randomly chosen (or appropriately fixed) element in Z_N^*, can compute $g^{2^{2^{t(n)}}} \bmod N$ is bounded by $\mu(n)$.*

We note that essentially the repeated squaring assumption has two security parameters, n and $t(n)$, where the former decides the size of the modulus and the maximal size $B(n)$ of the adversaries (such that factoring the modulus remains hard), and the latter decides the number $2^{t(n)}$ of repeated squaring needed to solve the puzzle by brute force, and the maximal depth $T(t(n))$ of the adversaries. The assumption says that the puzzle is hard for adversaries of depth up to $T(t(n))$ and size up to $B(n)$, even if the size of the adversary may be larger than $T(t(n))$ or even $2^{t(n)}$ (but still bounded by $B(n)$). Note also that the subexponential repeated squaring assumption implies the subexponential hardness of factoring.[4]

We remark that comparing with other subexponential assumptions (such as e.g., the subexponential DDH assumption), the subexponential repeated squaring assumption is milder in the sense that it is a search assumption instead of a decisional assumption. It also has a strong "win-win" flavor: Repeated squaring is a problem that arises naturally in the design of algorithms (e.g., any improvement on repeated squaring would yield improved efficiency for the verification of RSA-based signatures.) On the other hand, the subexponential repeated squaring assumption has a non-standard form in that the puzzle is easy to solve in depth $2^{t(n)}$, but hard to solve in depth $2^{t(n)^\varepsilon}$ and size more than $2^{t(n)}$ and below $B(n)$.

We finally mention that the time-lock puzzle needed for our construction can also be based on the existence of a parallel-time hard language and indistinguishability obfuscation (with subexponential security) by the work of Bitansky *et al.* [BGJ+16].

[4] The state-of-the-art factoring algorithm runs in 2^{n^ε} time for some constant ε. The subexponential hardness of factoring assumes that factoring is hard for 2^{n^μ} time adversaries for some smaller constant $\mu < \varepsilon$.

Towards Non-interactive Non-malleable Commitments. We also address the question of whether fully non-interactive (i.e., single-message) non-malleable commitments are possible. We show that if we replace the assumption of the existence of ZAPs (i.e., two-message witness indistinguishability) with non-interactive witness indistinguishable proofs (NIWI) [BOV03, GOS06, BP15], and the existence of families of collision-resistant hash functions for a *single*, collision-resistant hash function secure against *uniform* adversaries, [BP04, Rog06], then a slightly modified *non-interactive* version of our protocol satisfies concurrent non-malleability w.r.t. *uniform attackers*: Basically, the first message of our two-round protocol only contains the first message of the ZAP, and the index of the hash function, so by relying on a NIWI and a single hash function (secure against uniform subexponential-time attackers), the first message can be skipped.

Theorem 2 (Informal)**.** *Let T and B be two arbitrary subexponential functions. Assume the existence of non-interactive commitments, a NIWI, a uniform collision-resistant function, all with subexponential-security, and the existence of a (T, B)-time-lock puzzle. Then, there exists a one-message concurrent non-malleable commitment secure w.r.t. uniform polynomial-time adversaries.*

We leave open the question of whether we can get a non-interactive non-malleable commitment w.r.t. non-uniform attackers.

Achieving Chosen Commitment Attack Security. Canetti, Lin, and Pass [CLP10, LP12] strengthened the notion of concurrent non-malleability to security against Chosen Commitment Attacks (CCA) for commitments, analogous to the extensively studied notion of security against Chosen-Ciphertext Attacks for encryption schemes. Roughly speaking, a commitment scheme is said to be CCA-secure if commitments remain hiding even against attackers with access to an inefficient oracle, called the committed-value oracle, that "breaks" each commitment sent by an attacker using brute force and returns the (unique) committed value as soon as the commitment is completed. In particular, CCA-security implies that it is infeasible for an attacker to "maul" commitments to a set of values into commitments to a set of related values, even with the help of the committed-value oracle—which implies concurrent non-malleability. It was shown in several works [CLP10, LP12, Kiy14, GLP+15] that CCA-secure commitments are useful for constructing multi-party computation protocols with concurrent and composable security in the plain model from polynomial-time hardness assumptions. Furthermore, in a recent work [BHP17], 2-round CCA-secure commitments are further used for constructing round-optimal, 4-round, multi-party computation protocols secure in the stand-alone setting. We show that our two-round, and non-interactive non-malleable commitments, in fact, satisfy the stronger notion of CCA security.

Theorem 3 (Informal)**.** *The two-round non-malleable commitment scheme of Theorem 1 satisfies CCA-security, and the non-interactive non-malleable commitment scheme of Theorem 2 satisfies CCA-security w.r.t. uniform polynomial-time adversaries.*

A Remark on "Sub-subexponential" Security. Let us finally mention that although for the simplicity of notation we rely on subexponential hardness assumption, our actual proof reveals that we only need to rely on "sub-subexponential"[5] hardness assumption for all the primitives we rely on: namely, we only require security to hold w.r.t. attackers of size (and depth) $2^{n^{1/\log\log n}}$ (and in fact, even slightly less).

[5] We refer to $2^{n^{o(1)}}$ as a sub-subexponential function.

Why Time-Lock Puzzles? Our Ideas In a Nut Shell. In cryptography, the power, or *resource*, of attackers is usually measured by their running-time when represented as Turing machines, or equivalently by their circuit-size when represented as circuits. Time-lock puzzles, and more generally timed-release cryptography [May93, DN93, JJ99, Nak12, BN00], on the other hand, measure the resource of attackers by their parallel running-time or equivalently by their circuit-depth. Our 2-round non-malleable commitments crucially rely on the synergy between these two types of resources. The key idea is, instead of measuring the hardness of commitment schemes in a single "axis" of resource, measure the hardness in two axes, one refers to circuit-size and the other to circuit-depth. By doing so, we can construct a pair of commitment schemes $\mathsf{Com}_1, \mathsf{Com}_2$ that are simultaneously harder than the other, in different axes. In particular, Com_2 is harder in the axis of *circuit-size*, in the sense that Com_1 admits an extractor of size S while Com_2 is secure against all circuits of size S; on the other hand, Com_1 is harder in the axis of *circuit-depth*, in the sense that Com_2 admits an extractor of depth D (and some size S') while Com_1 is hiding against all circuits with depth D (and size S'). Such a pair of commitment schemes that are mutually harder than each other already has a weak flavor of non-malleability — no adversary can "maul" a Com_2 commitment to v into a Com_1 commitment to a related value, say $\tilde{v} = v + 1$, as otherwise one can extract $\tilde{v}$ in size S, which violates the hiding of Com_2 against S-size circuits. Similarly, no adversary can "maul" a Com_1 commitment into a Com_2 commitment, as otherwise, we can find $\tilde{v}$ in small depth D (and size S'), which violates the hiding of Com_1 against depth D circuits (of size S'). Next, we amplify this weak non-malleability to full-fledged non-malleability. More precisely, we transform the aforementioned commitment schemes, which are non-malleable w.r.t. short "tags" to that for much longer "tags" (explained below), while keeping two rounds.

1.2 Concurrent and Independent Work

A concurrent and independent, beautiful, work by Khurana and Sahai (KS) [KS17] also presents a construction of 2-round non-malleable commitments from subexponential hardness assumptions. The results, however, are incomparable, both in terms of assumptions, and also in terms of the achieved results (and use significantly different techniques).

In terms of results, our protocols satisfy *full* concurrent non-malleability, whereas the KS protocol only satisfies "bounded-concurrent" non-malleability—which is a weaker notion of concurrent non-malleability where the number of sessions is *a-priori bounded* by some pre-determined polynomial in the security parameter; in particular, the communication complexity of their protocol grows super linearly with the bound on the number of sessions, and the complexity assumptions they rely on need to be parametrized by it. Additionally, we also present a fully non-interactive protocol, whereas their technique appears to be inherently limited to two-round protocols.

In terms of assumptions, the key difference is that KS does not rely on time-lock puzzles but rather on the existence of certain 2-round secure two-party computation protocols (with super-polynomial-time simulation security); they also claim that such protocols can be constructed based on the subexponential DDH assumption, or the subexponential QR assumption. These assumptions are incomparable to the subexponential repeated squaring assumption, which as we mentioned above is also a very natural computational problem that has been extensively studied over the years. On a qualitative level, it is also a search assumption (and thus our construction of non-malleable commitments can be based on search assumptions), whereas the KS construction (due to the above DDH, or QR, assumption) relies on "decisional assumptions".

1.3 A Perspective: Non-Malleability from Hardness in Different Axes

In this work, our foremost idea is deriving non-malleability from hardness in different axes. While our particular instantiation uses commitments hard in the axis of circuit-size (or time) and commitments hard in the axis of circuit-depth (or parallel time), these are many other types of resources one can consider. For instance, the concurrent work by Khurana and Sahai [KS17] uses commitments extractable in certain time without rewinding, and rewinding does not help extraction (e.g. any non-interative commitments), and commitments extractable using rewinding, and is extremely hard to break without rewinding (they constructed such commitments using special 2-round two-party computation protocols). We can view the hardness axes involved in their work as 1) time for extraction without rewinding, and 2) time for extraction with rewinding. In a follow-up work by Bitansky and Lin [BL18] on constructing one-message zero-knowlege arguments and non-malleable commitments from keyless multi-collision resistant hash functions and other assumptions, they considered two axes: 1) time for extraction with probability 1 and 2) the probability of successful extraction in polynomial time. More precisely, they build $\mathsf{Com}_1, \mathsf{Com}_2$ such that the values committed using Com_2 can be extracted with probability 1 in time T, while Com_1 remains hiding in time T, whereas the probability that a polynomial-time extractor succeeds in extracting values from Com_2 is much smaller than that from Com_1. In another follow-up work [BDSK+18] on constructing non-malleable codes against bounded polynomial time tampering, they considered the axis of "BP-time" corresponding to time for extraction by probablistic Turing machine, and the axis of non-deterministic "(ND)-size" corresponding to time for extraction by NP circuits. We believe that there are more hardness axes and considering their synergy may lead to new applications.

1.4 Organization

In Section 2, we give a detailed overview of our approach for constructing 2-round non-malleable commitments. In Section 3, we provide preliminaries and definitions. Section 4 presents a family of basic commitment schemes that are mutually harder than each other at different axis, we call them size-robust, depth-robust and size-and-depth robust commitments. Using these basic commitment schemes, in Section 5, we construct a commitment scheme for short identities that satisfy a weaker notion of non-malleability that we formalize as non-malleability w.r.t. extraction. In Section 6, we present a non-malleability strengthening technique that lifts non-malleability w.r.t. extraction in the stand-alone setting to both non-malleability w.r.t. extraction and standard non-malleability in the concurrent setting. In Section 7, we present a transformation that increases the length of identities exponentially at the cost of loosing concurrent non-malleability. In Section 8, we construct 2-round non-malleable commitment scheme for n-bit identities, by iteratively applying the amplification technique in Sections 6 and 7 to the basic scheme in Section 5. Then in Section 9 we discuss the robust CCA-security of the 2-round non-malleable commitment scheme described in Section 8. Finally in Section 10, we show how to remove the first-message in our 2-round non-malleable and robust-CCA secure commitment from Section 8 when the attackers are restricted to be uniform Turing machines.

2 Overview

Every secure statistically binding commitment scheme is *hiding* against polynomial-sized circuits, while *extractable* by some exponential-sized circuit (such an extractor is guaranteed to exist since one can always find the committed value by brute force). In this work, we pay special attention to the *gap* between the "resources" of attackers and that of extractors. Moreover, we crucially rely on

the synergy between different resources — in particular, *circuit-size* and *circuit-depth*, which are captured by the following two basic types of commitment schemes:

Size-Robust Commitments are parametrized versions of classical commitments: An (S, S')-*size-robust commitment* is hiding against any size-$\mathsf{poly}(S)$ attackers, and extractable by some size-S' extractor, for an $S' = S^{\omega(1)}$ denoted as $S' >> S$, of *shallow* polynomial depth where S and S' are some function of the security parameter. For instance, such extractors can be implemented using the naïve brute force strategy of enumerating all possible decommitments, which is a time-consuming but highly-parallelizable task.

Depth-Robust Commitments are natural analogues of size-robust commitments, but with respect to the resource of circuit-depth. A (D, D')-*depth-robust commitment* is hiding against any depth-$\mathsf{poly}(D)$ circuits with size up to a large upper bound B, and extractable by some *size-D'* extractor for $B > D' >> D$ that necessarily has a depth super-polynomially larger than D. In this work, we consider a subexponential size upper bound $B = 2^{n^\varepsilon}$ for some constant $\varepsilon > 0$; for simplicity of exposition, we ignore this upper bound in the rest of this overview (see Section 4 for more detail).

Size-Robust Commitments from Subexponential Injective OWFs. The size-robust commitments we need (for specific relations between S and S') can essentially be instantiated using any off-the-shelf commitment schemes that are subexponentially secure, by appropriately scaling the security parameter to control the levels of security and hardness for extraction. Take the standard non-interactive commitment scheme from any injective one-way function f as an example: A commitment to a bit b is of the form $(f(r), h(r) \oplus b)$, consisting of the image $f(r)$ of a random string r of length n, and the committed bit b XORed with the hard-core bit $h(r)$. Assuming that f is subexponentially hard to invert, the commitment is hiding against all size-2^{n^ε} circuits for some constant $\varepsilon > 0$, while extractable in size 2^n (ignoring polynomial factors in n) and polynomial depth. By setting the security parameter n to $(\log S)^{1/\varepsilon}$, we immediately obtain a (S, S')-size robust commitment for $S' = 2^{\log S^{1/\varepsilon}}$.

Depth-Robust Commitments from Time-Lock Puzzles. Depth-robust commitments are naturally connected with cryptographic objects that consider parallel-time complexity, which corresponds to circuit-depth. When replacing subexponentially-hard one-way functions in the above construction with time-lock puzzles, we immediately obtain depth-robust commitments:

- To commit to a bit b, generate a puzzle puzz with a random solution s and a designated level of hardness t, and hide b using the Goldreich-Levin hard-core bit, producing $C = (\mathsf{puzz}, r, \langle r, s\rangle \oplus b)$ as the commitment.

- To decommit, the committer can simply reveal the puzzle solution s together with the random coins ρ used for generating the puzzle. The receiver verifies that the puzzle is honestly generated with solution s, and uses s to recover the committed bit b.

Since the time-lock puzzle solution s is hidden against adversaries in parallel-time $T(t)$ (and overall time $B(n)$), the commitments are hiding against depth-$T(t)$ adversaries (with size up to $B(n)$). Moreover, since the puzzles can be "forcefully" solved in time 2^t, the committed values can be extracted in size 2^t. This gives a $(T, 2^t)$-depth-robust commitment.[6]

[6] Binding follows from the injectivity of time-lock puzzles.

Next, we show how to compose the basic size-robust and depth-robust commitment schemes to overcome Pass's impossibility result on 2-round non-malleable commitments.

2.1 Towards Overcoming the Impossibility Result

In the literature, there are two formulations of non-malleable commitments, depending on whether the commitment scheme uses players' *identities* or not. The formulation with identities, adopted in this work, assumes that the players have identities of certain length ℓ, and that the commitment protocol depends on the identity of the committer, which is also referred to as the *tag* of the interaction. Non-malleability ensures that, as long as the tags of the left and right commitments are different (that is, the man-in-the-middle does not copy the identity of the left committer), no man-in-the-middle attacker can "maul" a commitment it receives *on the left* into a commitment of a related value it gives *on the right*. This is formalized by requiring that for any two values v_1, v_2, the values the man-in-the-middle commits to after receiving left commitments to v_1 or v_2 are indistinguishable. The other formulation without identities requires that, as long as the transcript of messages in the left and right commitments are not identical, the committed values must be computationally independent (formulated identically as above). It is known that these two formulations are equivalent when the length of the identities and that of the committed strings are polynomial.

The length ℓ of the tags can be viewed as a quantitative measure of how non-malleable a scheme is: An ℓ-bit tag non-malleable commitment gives a family of 2^ℓ commitment schemes — each with a hardwired tag — that are "mutually non-malleable" to each other. Therefore, the shorter the tags are, the easier it is to construct such a family. Full-fledged non-malleable commitments have tags of length equal to the security parameter $\ell = n$, and hence corresponds to a exponentially sized family. However, when the number of communication rounds is restricted to 2, Pass [Pas13] showed that even the weakest non-malleable commitment for just *1-bit tags*, corresponding to a size 2 family, cannot be reduced from falsifiable assumptions, via a polynomial-time black-box reduction.

One-Sided Non-Malleability via Complexity Leveraging. It is well known that *one-sided non-malleability* can be achieved easily via complexity leveraging. One-sided non-malleability only prevents mauling attacks when the tag of the left commitment is "larger than" the tag of the right commitment.[7] In the simple case of 1-bit tags, this requires the commitment for tag 1 (on the left) to be non-malleable w.r.t. the commitment for tag 0 (on the right), which holds if the tag-1 commitment is "harder" than the tag-0 commitment. For example, if the tag-1 commitment is (S_1, S_1')-size-robust while the tag-0 commitment is (S_0, S_0')-size-robust for some $S_0 << S_0' << S_1 << S_1'$, then one can extract the right committed value using a size-S_0' extractor, while the left committed value still remains hidden. Therefore, the right committed value must be (computationally) independent of the left. Similarly, we can also achieve one-sided non-malleability using depth-robust commitments, by using a (D_1, D_1')-depth robust commitment scheme for tag 1 and a (D_0, D_0')-depth robust commitment scheme for tag 0, for some $D_0 << D_0' << D_1 << D_1'$.

However, simple complexity leveraging is inherently limited to one-sided non-malleability, since when only one resource is considered, the tag-1 commitment cannot be both harder and easier than the tag-0 commitment.

[7] The choice that the left tag is smaller than the right tag is not important. One could also require the opposite, that is, the left tag is larger than the right tag. The limitation is that the design of the commitments depends on this arbitrary decision.

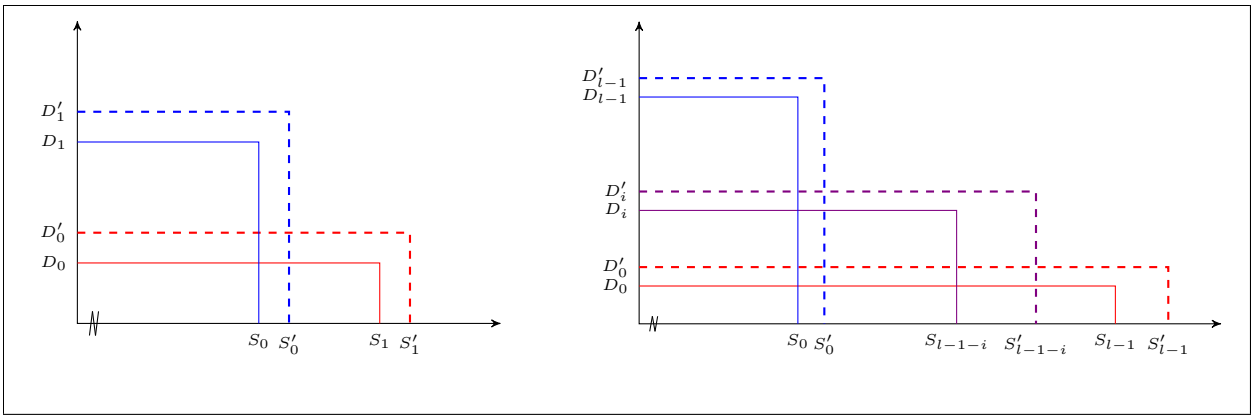


Figure 1: (left) A 1-bit tag based commitment scheme: The tag-0 (resp., tag-1) commitment scheme is hiding for circuits of depth below D_0 (resp., D_1) *OR* size below S_1 (resp., S_0), represented by the solid line joining D_0 (resp., D_1) and S_1 (resp., S_0). The tag-0 (resp., tag-1) commitment scheme admits an extractor of depth at most D'_0 (resp., D'_1) and size at most S'_1 (resp., S'_0). (right) This is a generalization of the 1-bit tag commitment scheme to $\log l$-bits tags, where for tag-i the commitment scheme is hiding for circuits of depth below D_i *OR* size below S_{l-1-i} and exhibits an extractor of depth at most D'_i and size at most S'_{l-1-i}.

Two Resources for (Two-Sided) Non-Malleability. Therefore, our key idea is using two resources to create two "axes", such that, the tag-1 commitment and tag-0 commitment are simultaneously "harder" than the other, but, with respect to different resources. This is achieved by combining the basic size-robust and depth-robust commitment schemes in the following simple way.

Basic 1-bit Tag Non-Malleable Commitment:
For some $D_0 << D'_0 << D_1 << D'_1 << S_0 << S'_0 << S_1 << S'_1$,

- a tag-0 commitment to a value v consists of commitments to two random, xor secret shares α, β of v, such that, $v = \alpha + \beta$, where the first share is committed under a (D_0, D'_0)-depth-robust commitment scheme and the second under a (S_1, S'_1)-size-robust commitment scheme, and

- a tag-1 commitment to v, on the other hand, uses a (D_1, D'_1)-depth-robust commitment scheme to commit to the first share and a (S_0, S'_0)-size-robust commitment scheme to commit to the second share.

Thus, the tag-1 commitment is harder w.r.t. circuit-depth, while the tag-0 commitment is harder w.r.t. circuit-size. Leveraging this difference, one can extract from a tag-0 commitment (on the right) without violating the hiding property of a tag-1 commitment (on the left), and vice versa — leading to two-sided non-malleability. More specifically, the committed values in a tag-0 commitment can be extracted in depth D'_0 and size S'_1 by extracting both secret shares from the size- and depth-robust commitments contained in it. Yet, adversaries with such depth and size cannot break the (D_1, D'_1)-depth-robust commitment contained in a tag-1 commitment; thus, the value committed to in the tag-1 commitment remains hidden. On the flip side, the committed value in a tag-1 commitment can be extracted in depth D'_1 and size S'_0, and, similarly, adversaries with such depth and size do not violate the hiding of a tag-0 commitment, due to the fact that the size-robust commitment contained in it is hiding against size-S_1 adversaries.

In summary, combining the two types of commitment schemes gives us depth-and-size robust commitment schemes: A $(D \vee S, D' \wedge S')$-robust commitment is hiding against circuits with depth below D *or* size below S, while extractable by some circuit with depth D' *and* size S', as illustrated in Figure 1 (left). In this language, a tag-0 commitment is $(D_0 \vee S_1, D'_0 \wedge S'_1)$-robust while a tag-1 commitment is $(D_1 \vee S_0, D'_1 \wedge S'_0)$-robust. They are mutually non-malleable, because the extractor for one falls into the class of adversaries that the other is hiding against.

The Subtle Issue of Over-Extraction. The above argument captures our key idea, but is overly-simplified. It implicitly assumes that the size- and depth-robust commitments are extractable in the perfect manner: 1) Whenever a commitment is valid, in the sense that there exists an accepting decommitment, the extractor outputs exactly the committed value, otherwise, 2) when the commitment is invalid, it outputs $\perp$. Such strong extractability ensures that to show non-malleability – the right *committed* value is independent of the left committed value, it suffices to show that the right *extracted* value is independent of the left committed value, as argued above. On the other hand, suppose that property 2) does not hold, that is, when the commitment is invalid, the extractor may output arbitrary values – this is known as *over-extraction*. In this case, we can no longer argue the independence of the right committed value based on the independence of the right extracted value. For instance, the extracted value $\tilde{v}$ may not change as the left committed value changes, but the right committed value may have switched from $\tilde{v}$ to $\perp$.

However, our depth-robust commitments from time-lock puzzles do not satisfy such strong extractability.[8] In particular, they are subject to over-extraction. Over-extraction traces back to the fact that only *honestly generated* time-lock puzzles (*i.e.*, in the domain of the puzzle generation algorithm) are guaranteed to be solvable in certain time. There is no guarantee for ill-generated puzzles, and no efficient procedure for deciding whether a puzzle is honestly generated or not. Observe that this is the case for the time-lock puzzles proposed by Rivest, Shamir, and Wagner [RSW96], since given a puzzle $(s + g^{2^{2^t}} \bmod N,\ N)$ one can extract s using 2^t squaring modular N, but cannot obtain a proof that N is a valid RSA-modulus; this is also the case for the other puzzle construction [BGJ+16]. As a result, the extractor of our depth-robust commitments that extracts committed values via solving time-lock puzzles, provides no guarantees when commitments are invalid.

This means that our basic 1-bit tag commitment scheme is over-extractable, and the argument above that reasons about the right extracted value fails to establish non-malleability. Nevertheless, the basic scheme does satisfy a variant of non-malleability that we call *non-malleability w.r.t. extraction*, which ensures that the value *extracted* from the right commitment is independent of the left committed value.[9] When a commitment scheme is perfectly-extractable, this new notion is equivalent to standard non-malleability (w.r.t. commitment), but with over-extraction, it becomes incomparable. The issue of over-extraction has appeared in the literature (*e.g.*, [Wee10, Kiy14]), standard methods for dealing with over-extraction requires the committer to additionally prove the validity of the commitment it sends, using for instance zero-knowledge protocols or cut-and-choose techniques. However, these methods take more than 2 rounds of interaction, and do not apply here.

[8] Our size-robust commitments from injective one-way functions do satisfy such strong extractability.

[9] Our notion of non-malleability w.r.t. extraction is inspired from the notion of non-malleability w.r.t. extraction defined by Wee [Wee10]. Furthermore, our notion can be viewed as a special case of the notion of non-malleability w.r.t. replacement defined by Goyal [Goy11], in the sense that the replacer in Goyal's definition is fixed to the over-extractor of the commitment scheme. The benefit of doing so is that we know exactly the complexity of the extractor, which is useful in the rest of the construction.

2.2 Full-Fledged Non-Malleable Commitments

At this point, we face two challenges towards constructing full-fledged non-malleable commitments:

- *Challenge 1:* We need to go from non-malleability w.r.t. extraction to non-malleability w.r.t. commitment in 2 rounds. Resolving this challenge would give a 2-round 1-bit tag non-malleable commitment scheme.

- *Challenge 2:* The next challenge is going beyond two tags, towards supporting an exponential 2^n number of tags.

  It is easy to generalize our basic 1-bit tag commitment scheme to handle arbitrary l tags, if there exists a "ladder" of l commitment schemes with increasing levels of depth-robustness, and another "ladder" of l schemes with increasing levels of size-robustness. Concretely, the i'th schemes are respectively (D_i, D'_i)-depth robust and (S_i, S'_i)-size robust, for some

  $$\cdots << D_i << D'_i << \cdots << D_{l-1} << D'_{l-1} << S_0 << S'_0 << \cdots << S_i << S'_i << \cdots .$$

  A commitment with tag $i \in \{0, \cdots, l-1\}$ combines the i'th (D_i, D'_i)-depth-robust scheme and the $(l-i-1)$'th (S_{l-i-1}, S'_{l-i-1})-size-robust scheme to commit to a pair of secret shares of the committed value. This gives a family of l mutually non-malleable commitment schemes, as illustrated in Figure 1 (right).

  To directly obtain full-fledged non-malleable commitments, we need an exponential number of levels $l = 2^n$ of depth- and size-robustness, which is, however, impossible from the underlying assumptions. From generic subexponentially hard, say 2^{n^ε} hard, injective one-way functions, we can instantiate at most $O(\log \log n)$ levels of size-robustness. (This is because if we instantiate the i'th size-robust commitment using the one-way functions with security parameter n_i, the commitment is hiding for adversaries of size $S_i = \mathsf{poly}(2^{n_i^\varepsilon})$, and can be broken by adversaries of size $S'_i = \mathsf{poly}(2^{n_i})$. Then, ensuring $S'_{i-1} << S_i$ entails that $n_{i-1}^{1/\varepsilon} < n_i$, and hence $n_0^{1/\varepsilon^i} < n_i$. Since n_i also needs to be polynomial in the global securty parameter n, we have $i = O(\log \log n)$.) Similarly, from subexponentially parallel-time hard time-lock puzzles, we can instantiate $O(\log \log n)$ levels of depth-robustness. Therefore, we need to amplify the number of tags.

We address both challenges using a single transformation.

2-Round Tag Amplification Technique: We present a transformation that converts a 2-round l-tag commitment scheme that is non-malleable w.r.t. extraction, into a 2-round 2^{l-1}-tag commitment scheme that is both non-malleable w.r.t. extraction and w.r.t. commitment. The output protocol can be further transformed to achieve concurrent non-malleability.

With the above transformation, we can now construct full-fledged non-malleable commitment. Start from our basic scheme for a constant $l_0 = O(1)$ number of tags that is non-malleable w.r.t. extraction; apply the tag-amplification technique *iteratively for* $m = O(\log^* n)$ *times* to obtain a scheme for $l_m = 2^n$ tags that is both non-malleable w.r.t. extraction and w.r.t. commitment.

Previously, similar tag-amplification techniques were presented by Lin and Pass in [LP09] and by Wee in [Wee10]. Our transformation follows the same blueprint, but differ at two important aspects. First, our transformation starts with and preserves non-malleability w.r.t. extraction,

which is not considered in their work. Second, their amplification techniques incur a constant additive overhead in the round complexity of the protocol, whereas our transformation keeps the number of rounds invariant at 2. To do so, our amplification step combines ideas from previous works with the new idea of using our depth-and-size robust commitments to create different 2-round sub-protocols that are mutually "non-malleable" when executed in parallel, in the sense that the security of one sub-protocol remains intact even when the security of another is violated by force.

Our 2-Round Tag-Amplification Technique in More Detail. Similar to [LP09, Wee10], the transformation proceeds in two steps:

- First, amplify the security of a scheme from (*one-one*) non-malleability w.r.t. extraction to *one-many* non-malleability w.r.t. extraction and commitment, which, following a proof in [LPV08], implies *concurrent* (or many-many) non-malleability w.r.t. extraction and commitment. (This is why our final protocol can be made concurrently non-malleable.) Here, one-many and concurrent non-malleability w.r.t. extraction or commitment naturally generalize standard non-malleability to the setting where the man-in-the-middle concurrently receives one or many commitments on the left and gives many commitments on the right, and ensures that the joint distribution of the values extracted from or committed in right commitments is independent of the value(s) committed in the left commitments.

- Next, apply the "log-n trick" by Dolev, Dwork and Naor [DN00] to amplify the number of tags supported from l to 2^{l-1} at the price of losing concurrent security, yielding a protocol that is (*one-one*) non-malleable w.r.t. extraction and commitment.

The main technical challenges lie in the first step. We briefly review the LP [LP09] approach. At a high-level, they construct one-many non-malleable commitment following the Fiege-Lapidot-Shamir paradigm [FLS90]: The receiver starts by setting up a *hidden* "trapdoor" t. The sender commits to a value v using an arbitrary (potentially malleable) 2-message commitment scheme, followed by committing to 0^n using a (one-one) non-malleable commitment and proving using *many* witness-indistinguishable proofs of knowledge (WIPOK) that either it knows a decommitment to v *or* it knows a decommitment of the non-malleable commitment to the trapdoor t; the former, called the honest witness, is used by the honest committer, while the latter, called the fake witness, is used for simulation.

The LP protocol arranges all components — the trapdoor-setup, commitment to v, non-malleable commitment (for trapdoor), and every WIPOK — *sequentially*. To compress the protocol into 2 rounds, we run all components in *parallel*, and replace multiple WIPOK proofs with a single 2-round ZAP proof.

Unfortunately, arranging all components in parallel renders the proof of one-many non-malleability in LP invalid. They designed a sequence of hybrids in which different components in the (single) left interaction are gradually switched from being honestly generated to simulated, while maintaining two invariants regarding the (many) right interactions. First, the *soundness* condition states that the man-in-the-middle never commits to a trapdoor in any right interaction. Second, in every right interaction, there is always a WIPOK that can be rewound to extract the value committed to in this interaction, without rewinding the left component being changed; the value extracted must be a valid decommitment since the fake witness does not exist by the soundness invariant — this establishes *strong extractability*. The second invariant is true because the LP protocol contains sufficiently many sequential WIPOKs so that there is always a proof that does not interleave with the left-component being changed. The first invariant, on the other hand, relies not only on the

non-malleability of the input commitment scheme, but also on its "robustness" to other components that have a small fixed k number of rounds (such as 2-message commitment and WIPOK). The robustness captures "non-malleability" w.r.t. other protocols, and is achieved by embedding more than k rewinding slots in the input commitment scheme.

In our 2-round protocol, we cannot afford to have many rewinding slots for extraction, nor for establishing non-malleability between different components. Naturally, we resort to our size-and-depth robust commitments, which can be made mutually non-malleable w.r.t. extraction by setting the appropriate profiles of size-and-depth robustness. We embed a family of 4 such commitments in different components of the protocol, and mimic the LP proof in the following (overly-simplified) manner: In every hybrid, in the left interaction, either a size-and-depth robust commitment or the non-malleable commitment is changed, while on the right, committed values are extracted from a *different* size-and-depth robust commitment or from the non-malleable commitment. (Note that since we now extract values from commitments instead of from WI proofs, we no longer need many WIPOKs and a single ZAP suffices.)

To show that the left interaction remains indistinguishable despite the extraction, we rely on the mutual non-malleability of the size-and-depth robust schemes, but also need the non-malleable commitment and the size-and-depth robust commitments to be mutually non-malleable, which unfortunately does not hold.

Let us explain. It turns out that our basic non-malleable commitment schemes for short tags, and all intermediate schemes produced by the tag-amplification technique are only secure against circuits with *both* bounded-size *and* bounded-depth. In contrast, the depth-and-size robust commitments are secure against circuits with *either* bounded-size *or* bounded-depth. This qualitative difference in adversarial circuit classes prevents them from being mutually non-malleable. To get around this, we instead rely on a "cycle of non-malleability" that consists of the non-malleable commitment scheme and two depth-and-size robust commitment schemes, satisfying that the first scheme is non-malleable to the second, the second non-malleable to the third, and the third to the first. Such a cycle turns out to be sufficient for our proof to go through.

One final technicality is that in order to create the cycle of non-malleability, the hardness of the two size-and-depth robust commitments must be set appropriately according to that of the non-malleable commitment scheme. Furthermore, the non-malleable commitment scheme produced by the above transformation has weaker security than the input scheme. As a result, to iteratively apply the tag-amplification technique for $O(\log^* n)$ times, we need $O(\log^* n)$ levels of depth- and size-robustness. This can be easily instantiated using subexponentially secure non-interactive commitment schemes and time-lock puzzles as stated in Theorem 1. See Section 6 for more details on our tag amplification and its security proof.

2.3 Extensions

Finally, we briefly mention two extensions. First, our two-round non-malleable commitment scheme can be made non-interactive, at the price of becoming only concurrent non-malleable against attackers that are uniform Turing machines. Second, we show that our two-round non-malleable commitment scheme (and its non-interactive version resp.) in fact satisfies the stronger notion of Chosen Commitment Attack (CCA) security (against uniform Turing machines resp.).

Non-Interactive Non-Malleable Commitments w.r.t. Uniform Attackers. For the first extension, observe that the only step in our construction that requires 2 rounds is the non-malleability strengthening step in the tag-amplification technique. (The basic non-malleable scheme

for a constant number of tags are non-interactive and the log-n trick in the tag-amplification technique is round-preserving.) The non-malleability strengthening step produces 2-round protocols, where the first message is from the receiver and consists of i) the first message of a 2-round WI proof, ii) a randomly sampled function from a family of collision resistant hash functions secure against non-uniform attackers, and iii) the first message of the input (one-one) non-malleable commitment scheme if it has 2 rounds. To remove the first message we can simply replace 2-round WI proofs with non-interactive WI proofs (NIWIs), and fix a single hash function (instead of a family). However, since a single hash function can only be collision resistant to attackers that are uniform Turing machines, the resulting non-interactive commitment scheme is only concurrent non-malleable against uniform adversaries. See Section 10 for more details.

CCA-secure Commitments. CCA-security strengthens the notion of concurrent non-malleability in ways similar to how Chosen Ciphertext Attack secure encryption strengthens non-malleable encryption. Roughly speaking, CCA-security requires that no man-in-the-middle attacker can distinguish commitments to different values on the left, even if it has access to a committed-value oracle, which breaks every commitment the attacker sends on the right (except the left commitment), and returns the unique committed value as soon as the right interaction ends. Our 2-round concurrent non-malleable commitments are in fact CCA-secure. To see this, it suffices to argue that the non-malleability strengthening step in the tag-amplification technique produces CCA-secure commitments, as the final 2-round protocol is produced by this procedure. Recall that to show the concurrent non-malleability of the resulting 2-round protocol, we built a sequence of hybrids, where different components in the left commitment are changed one by one, while the right committed values are extracted by breaking different components in right commitments. The indistinguishability of neighboring hybrids follows from the mutual non-malleability of the component being broken on the right, and the component being changed on the left. We observe that this argument can be easily changed to prove CCA security. The only modification to the hybrids is simulating the committed-value oracle for the attacker by sending it the values extracted from the right commitments. The mutual non-malleability of different components still guarantees the indistinguishability of the hybrids, now with committed-value oracles. There are still some subtleties in the proof; see Section 9 for more details.

3 Preliminaries

3.1 Basic Notation

We denote the security parameter by n. For $n \in \mathbb{N}$, by $[n]$ we denote the set $\{1, \ldots, n\}$. If v is a binary string then $|v|$ denotes the length of the string and $v[i]$ is the ith bit of v, for $0 \leq i \leq |v| - 1$. We use $||$ as the string concatenation operator. We identify strings $p \in \{0,1\}^t$ with an index in $[2^t]$. For any probability distribution D, $x \leftarrow D$ denotes sampling an element from the distribution D and assigning it to x. However, for a finite set Q, $x \leftarrow Q$ denotes sampling an element from the set Q uniformly and randomly, and assigning it to x. We model algorithms as uniform TMs. We use the abbreviation PPT to denote probabilistic-polynomial time. $\mathcal{P}/\text{poly}$ is the set of all non-uniform polynomial size circuits. We say that a function $\nu : \mathbb{N} \to \mathbb{R}$ is negligible, if for every constant $c > 0$ and for all sufficiently large $n \in \mathbb{N}$ we have $\nu(n) < n^{-c}$. For functions d, S defined over $\mathbb{N}$, we say that $d < S$ (resp. $d \leq S$) if for all sufficiently large $n \in \mathbb{N}$, $d(n) < S(n)$ (resp. $d(n) \leq S(n)$). Furthermore, we say that $d << S$ if for every polynomial poly, $\mathsf{poly}(d) < S$.

3.2 Circuit Classes

We define the following circuit classes which are going to be used throughout this work. For the following definitions, consider $n \in \mathbb{N}$ and let d, S and S^* be some non-decreasing functions defined on $\mathbb{N}$ such that $d \leq S << S^*$.

Definition 1 (Depth $\wedge$ size-restricted circuits)**.** *$\mathcal{C}^{\wedge}_{d,S}$ is the set of all non-uniform circuits $C = \{C_n\}_{n\in\mathbb{N}}$ such that there exists a polynomial* poly *such that for all sufficiently large $n \in \mathbb{N}$,*

$$\begin{aligned} & \mathsf{dep}(C_n) < \mathsf{poly}(d(n)) \\ \textit{and} \quad & \mathsf{size}(C_n) < \mathsf{poly}(S(n)) \ , \end{aligned}$$

where $\mathsf{dep}(C_n)$ and $\mathsf{size}(C_n)$ denote the depth and the size of the circuit C_n respectively.

Throughout this work, we only consider circuits of sub-exponential size. In particular, all such circuits have size significantly lesser than 2^{n^ε} for some $0 < \varepsilon < 1$. For generality, we let S^* to denote some pre-defined upper bound on the size of any circuits considered in this work. Furthermore, when we are only concerned with restricting the depth of the circuits, whose size can be as large as the upperbound $\mathsf{poly}(S^*)$ for any polynomial poly, we simply refer to the circuit class $\mathcal{C}^{\wedge}_{d,S^*}$ as $\mathcal{C}_d$.

Definition 2 (Depth-restricted circuits)**.** *$\mathcal{C}_d$ is the set of all non-uniform circuits $C = \{C_n\}_{n\in\mathbb{N}}$ such that there exists a polynomial* poly *such that for all sufficiently large $n \in \mathbb{N}$,*

$$\begin{aligned} & \mathsf{dep}(C_n) < \mathsf{poly}(d(n)) \\ \textit{and} \quad & \mathsf{size}(C_n) < \mathsf{poly}(S^*(n)) \ . \end{aligned}$$

Definition 3 (Depth $\vee$ size-restricted circuits)**.** *$\mathcal{C}^{\vee}_{d,S}$ is the set of all non-uniform circuits $C = \{C_n\}_{n\in\mathbb{N}}$ such that either $C \in \mathcal{C}_d$ or $C \in \mathcal{C}_S$.*

Remark 1. *The classes of circuits $\mathcal{C}$ (namely, $\mathcal{C}_d$,$\mathcal{C}^{\vee}_{d,S}$ and $\mathcal{C}^{\wedge}_{d,S}$) considered in this work are such that $S \geq d >> n$, that is, all d's and S's are super-polynomials. For such classes $\mathcal{C}$, composing any circuit $C \in \mathcal{C}$ with a circuit $P \in \mathcal{P}/\mathrm{poly}$ results in a circuit C' which is also in the class $\mathcal{C}$. Therefore, we say that the circuit class $\mathcal{C}$ is closed under composition with $\mathcal{P}/\mathrm{poly}$. This fact is going to be important in the rest of this work.*

Below, we define standard cryptographic primitives w.r.t. a general circuit class $\mathcal{C}$, requiring that any adversary in $\mathcal{C}$ has negligible advantage in breaking the security of the primitive. When $\mathcal{C} = \mathcal{P}/\mathrm{poly}$, we say that the primitive is computationally secure and when $\mathcal{C}$ is the set of non-uniform circuits whose size is bounded by 2^{n^ε} for some constant $\varepsilon < 1$, we say that the primitive is subexponentially secure.

3.3 Indistinguishability and One-wayness

Definition 4 ($\mathcal{C}$-indistinguishability)**.** *Two distribution ensembles $\{A_n\}_{n\in\mathbb{N}}$ and $\{B_n\}_{n\in\mathbb{N}}$ are said to be $\mathcal{C}$-indistinguishable, if for every non-uniform circuit $D = \{D_n\}_{n\in\mathbb{N}} \in \mathcal{C}$, there exists a negligible function $\nu(\cdot)$ such that for every $n \in \mathbb{N}$:*

$$\left|\mathsf{Pr}\left[a \leftarrow A_n : D_n(a) = 1\right] - \mathsf{Pr}\left[b \leftarrow B_n : D_n(b) = 1\right]\right| \leq \nu(n) \ .$$

Definition 5 ($\mathcal{C}$-unpredictability)**.** *Let $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$ be two ensembles of countable sets. Let $D = \{D_n\}_{n\in\mathbb{N}}$ be a distribution ensemble such that for every $n \in \mathbb{N}$, D_n is a distribution over pairs $(x, y) \in X_n \times Y_n$. We say that D is $\mathcal{C}$-unpredictable w.r.t. (X, Y) if for every non-uniform circuit $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ there exists a negligible function $\nu(\cdot)$ such that for every $n \in \mathbb{N}$,*

$$\mathsf{Pr}[(x, y) \leftarrow\!\!\$\, D_n, x' \leftarrow A_n(y) : x = x'] \leq \nu(n) \ .$$

Definition 6 (One-way functions)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is called a $\mathcal{C}^{\wedge}_{S,S}$-secure one-way function (OWF) if the following hold:*

1. *There exists a deterministic polynomial-time algorithm that on input s in the domain of f outputs $f(s)$.*
2. *For every $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}^{\wedge}_{S,S}$ there exists a negligible function $\nu(\cdot)$ such that for every $n \in \mathbb{N}$,*

$$\mathsf{Pr}\left[s \leftarrow \{0,1\}^n, s' \leftarrow A_n(f(s)) : f(s') = f(s)\right] \leq \nu(S(n)) \ .$$

As a short-hand, we will sometimes refer to $\mathcal{C}^{\wedge}_{S,S}$-secure one-way function as S-secure one-way function. In this work, we will use a one-way function that is injective and is subexponentially secure. That is, we assume the existence of a $\mathcal{C}^{\wedge}_{S,S}$-secure injective one-way function where $S = 2^{n^{\varepsilon}}$ for some $0 < \varepsilon < 1$.

Definition 7 (Hardcore functions)**.** *Let D be a distribution ensemble over pair (X, Y) of ensembles of countable sets. A function $h : X \to \{0,1\}$ is a $\mathcal{C}$-hardcore predicate of D if the following hold:*

1. *There exists a deterministic polynomial-time algorithm that on input $x \in X$ outputs $h(x)$.*
2. *For every $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ there exists a negligible function $\nu(\cdot)$ such that for every $n \in \mathbb{N}$,*

$$\mathsf{Pr}\left[(x, y) \leftarrow D_n, b \leftarrow A_n(y) : b = h(x)\right] \leq \frac{1}{2} + \nu(n) \ .$$

Theorem 4 (Golreich-Levin Hardcore Bit)**.** *Let D be a $\mathcal{C}$-unpredictable distribution ensemble over (X, Y) such that there exists a polynomially bounded function r such that for every $n \in \mathbb{N}$, $X_n \subseteq \{0,1\}^{r(n)}$. Let D' be the following distribution ensemble,*

$$\{((x, z), (y, z)) : (x, y) \leftarrow D_n, z \leftarrow \{0,1\}^{r(n)}\}_{n\in\mathbb{N}} \ .$$

And let $h : X \times \{0,1\}^r \to \{0,1\}$ be the function such that for every $(x, z) \in X \times \{0,1\}^r$, $h((x, z)) = \langle x \cdot z\rangle$. Then, D' is $\mathcal{C}$-unpredictable over $(X \times \{0,1\}^r, Y \times \{0,1\}^r)$ and h is a $\mathcal{C}$-hardcore predicate of D'.

Remark 2. *Goldreich and Levin [GL89] show that for any adversary $A \in \mathcal{C}$ that breaks the hardcoreness of h w.r.t. D' with probability $1/2 + \varepsilon(n)$ there exists an adversary B that breaks unpredictability of D where*

$$\mathsf{size}(B) \leq \mathsf{poly}(n/\varepsilon^2) \cdot \mathsf{size}(A) \ ; \ \mathsf{dep}(B) \leq \mathsf{poly}(n/\varepsilon^2) \cdot \mathsf{dep}(A) \ .$$

Since, $\varepsilon = 1/p(n)$ for some polynomial p the reduction blows up the size/depth of B over size/depth of A by only a $\mathsf{poly}(n)$ factor. Therefore, if $A \in \mathcal{C}$ then $B \in \mathcal{C}$ which then contradicts the $\mathcal{C}$-unpredictability of D.

3.4 Witness Relation, ZAP and NIWI

Definition 8 (Witness Relation)**.** *A witness relation or relation (for short) for a language $L \in \mathcal{NP}$ is a binary relation $\mathcal{R}_L$ that is polynomially bounded, polynomial time recognizable and characterizes L by $L = \{x : \exists w \text{ s.t. } (x, w) \in \mathcal{R}_L\}$.*

We say that w is a witness for the membership of $x \in L$ if $(x, w) \in \mathcal{R}_L$. We will also let $\mathcal{R}_L(x)$ denote the set of witnesses for the membership of $x \in L$; that is, $\mathcal{R}_L(x) = \{w : (x, w) \in \mathcal{R}_L\}$.

ZAPs are two-message public coin witness indistinguishable proofs defined as follows.

Definition 9 (ZAP [DN00])**.** *A pair of algorithms $(\mathcal{P}, \mathcal{V})$, where $\mathcal{P}$ is* PPT *and $\mathcal{V}$ is (deterministic) polytime, is a $\mathcal{C}$-*ZAP *for an $\mathcal{NP}$ relation $\mathcal{R}_L$ if it satisfies:*

1. *Completeness: There exists a polynomial $l(\cdot)$ such that for every $(x, w) \in \mathcal{R}_L$,*

$$\mathsf{Pr}\left[r \leftarrow \{0,1\}^{l(|x|)}, \pi \leftarrow \mathcal{P}(x, w, r) : \mathcal{V}(x, \pi, r) = 1\right] = 1 \ .$$

2. *Adaptive soundness: There exists a negligible function $\nu(\cdot)$ such that for every malicious (potentially unbounded) prover $\mathcal{P}^*$ and every $n \in \mathbb{N}$,*

$$\mathsf{Pr}\left[r \leftarrow \{0,1\}^{l(n)}, (x, \pi) \leftarrow \mathcal{P}^*(r) : x \in \{0,1\}^n \setminus L \wedge \mathcal{V}(x, \pi, r) = 1\right] \leq \nu(n).$$

3. *$\mathcal{C}$-witness indistinguishability: For any sequence $\{(x_n, w_n^1, w_n^2, r_n)\}_{n\in\mathbb{N}}$ such that for every $n \in \mathbb{N}$, $x_n \in L \cap \{0,1\}^n$, $w_n^1, w_n^2 \in \mathcal{R}_L(x_n)$ and $r_n \in \{0,1\}^{l(n)}$, the following ensembles are $\mathcal{C}$-indistinguishable:*

$$\{\pi_1 \leftarrow \mathcal{P}(x_n, w_n^1, r_n) : (x_n, w_n^1, w_n^2, \pi_1, r_n)\}_{n\in\mathbb{N}} \ ,$$
$$\{\pi_2 \leftarrow \mathcal{P}(x_n, w_n^2, r_n) : (x_n, w_n^1, w_n^2, \pi_2, r_n)\}_{n\in\mathbb{N}} \ .$$

Throughout this work, we will refer to the first message r of ZAP as a_{ZAP} and the second message together with the statement (π, x) as b_{ZAP}.

Dwork and Naor [DN00] were the first to construct a ZAP from certified trapdoor permutations [BY96]. They also showed that ZAP for $L \in \mathcal{NP}$ can be based on the weaker assumption of the existence of NIZKs for L.

Theorem 5. *If there exists a $\mathcal{C}$-secure family of certified trapdoor permutations then there exists a $\mathcal{C}$-*ZAP*.*

Furthermore, Bitansky and Paneth [BP15] construct ZAP based on the existence of indistinguishability obfuscation (iO) for a certain family of polysize circuits and one-way functions.

NIWIs are non-interactive witness-indistinguishable proofs.

Definition 10 (NIWI [BOV03])**.** *A pair of algorithms $(\mathcal{P}, \mathcal{V})$ where $\mathcal{P}$ is* PPT *and $\mathcal{V}$ is (deterministic) polytime, is a $\mathcal{C}$-*NIWI *for an $\mathcal{NP}$ relation $\mathcal{R}_L$ if it satisfies:*

1. *Completeness: For every $(x, w) \in \mathcal{R}_L$,*

$$\mathsf{Pr}\left[\pi \leftarrow \mathcal{P}(x, w) : \mathcal{V}(x, \pi) = 1\right] = 1 \ .$$

2. *Soundness:* *For every* $x \notin L$ *and* $\pi \in \{0,1\}^{\mathsf{poly}(|x|)}$*:*

$$\mathsf{Pr}\left[\mathcal{V}(x,\pi)=1\right]=0 \ .$$

3. $\mathcal{C}$*-witness indistinguishability:* *For any sequence* $\{(x_n, w_n^1, w_n^2)\}_{n\in\mathbb{N}}$ *such that for every* $n \in \mathbb{N}$, $x_n \in L \cap \{0,1\}^n$, $w_n^1, w_n^2 \in \mathcal{R}_L(x_n)$, *the following ensembles are* $\mathcal{C}$*-indistinguishable:*

$$\{\pi_1 \leftarrow \mathcal{P}(x_n, w_n^1) : (x_n, w_n^1, w_n^2, \pi_1)\}_{n\in\mathbb{N}} \ ,$$
$$\{\pi_2 \leftarrow \mathcal{P}(x_n, w_n^2) : (x_n, w_n^1, w_n^2, \pi_2)\}_{n\in\mathbb{N}} \ .$$

Dwork and Naor [DN00] showed the existence of a non-uniform non-constructive NIWI which can be based on their ZAP construction by fixing the first message non-uniformly. Building on their work, Barak, Ong and Vadhan [BOV03] de-randomize the ZAP verifier in [DN00] to give the first NIWI construction. They base their de-randomization technique on the existence of a function in $Dtime(2^{O(n)})$ with non-deterministic circuit complexity $2^{\Omega(n)}$. The ZAP construction from [BP15] can also be de-randomized under the same assumption. Furthermore, Groth, Ostrovsky and Sahai [GOS06] construct a NIWI based on the decisional linear assumption for bilinear groups.

Theorem 6. *We base the existence of* NIWI *on either of the following assumptions:*

1. *If decisional linear assumption holds for the elliptic curve based bilinear groups in [BF03] against all circuits in class* $\mathcal{C}$ *then there exists a* $\mathcal{C}$-NIWI.

2. *If* $\mathcal{C}$*-ZAPs exist and there exists a function in the class* $Dtime(2^{O(n)})$ *with non-deterministic circuit complexity* $2^{\Omega(n)}$ *then there exists a* $\mathcal{C}$-NIWI.

3.5 Commitment Schemes

Definition 11 (Commitment scheme)**.** *A commitment scheme* $\langle C, R\rangle$ *consists of a pair of interactive* PPT *TMs* C *and* R *with the following properties:*

1. *The commitment scheme has two stages: a commit stage and a reveal stage. In both stages,* C *and* R *receive as common inputs* 1^n *and* $1^{\alpha(n)}$ *and* C *additionally receives a private input* $v \in \{0,1\}^{\alpha(n)}$ *where* $n \in \mathbb{N}$ *is the security parameter and* $\alpha(\cdot)$ *is some polynomially bounded function.*[10]

2. *The commit stage results in a joint output* c*, called the commitment, a private output for* C*,* d*, called the decommitment string. Without loss of generality,* c *can be the full transcript of the interaction between* C *and* R *including the common input* 1^n *and* $1^{\alpha(n)}$*. Let* $n_c = n_c(n, \alpha(n))$ *denote the maximal length of the commitment generated by* $\langle C, R\rangle$ *while committing to an* $\alpha(n)$*-bit value on security parameter* n*.*

3. *In the reveal stage, committer* C *sends the pair* (v, d) *to the receiver* R*, and* R *decides to accept or reject the decommitment* (v, d) *deterministically according to an efficiently computable function* Open*; that is,* R *accepts iff* $\mathsf{Open}(c, v, d) = 1$*.*

4. *If* C *and* R *do not deviate from the protocol, then* R *should accept with probability 1 in the reveal stage.*

[10] For notational convenience we will usually drop the length of the value v being committer, that is, $1^{\alpha(n)}$ from the common input.

Furthermore, we say that a commitment c is valid, if there exists a string $v \in \{0,1\}^{\alpha(n)}$ and a decommitment string d such that $\mathsf{Open}(c, v, d) = 1$.

Next we define the binding and hiding property of a commitment scheme.

Definition 12 (Statistical binding)**.** *A commitment scheme $\langle C, R\rangle$ is statistically binding if for every polynomially bounded function $\alpha(\cdot)$ and for any committer C^* possibly unbounded, there exists a negligible function $\nu(\cdot)$ such that C^* succeeds in the following game with probability at most $\nu(n)$:*

On security parameter 1^n, C^* first interacts with R in the commit stage to produce a commitment c. Then C^* outputs two decommitments (v_0, d_0) and (v_1, d_1), and succeeds if $v_0, v_1 \in \{0,1\}^{\alpha(n)}$, $v_0 \neq v_1$ and R accepts both as decommitments of c.

Furthermore, a commitment scheme is perfectly binding if the probability that C^* succeeds in the above game is 0.

We define the value of any commitment through a function val, that takes as input an arbitrary commitment c and outputs v if c is valid and there exists exactly one value $v \in \{0,1\}^{\alpha}$ such that $\mathsf{Open}(c, v, d) = 1$ for some d, otherwise it outputs $\perp$. Note that such a function val may not be efficiently computable.

Definition 13 ($\mathcal{C}$-hiding)**.** *A commitment scheme $\langle C, R\rangle$ is $\mathcal{C}$-hiding if for every polynomially bounded function $\alpha(\cdot)$ and for every non-uniform circuit $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ there exists a negligible function $\nu(\cdot)$ such that A succeeds in the following game with probability at most $\frac{1}{2} + \nu(n)$:*

For security parameter 1^n, A_n outputs a pair of values $v_0, v_1 \in \{0,1\}^{\alpha(n)}$. C on input v_b, where b is a randomly chosen bit, interacts with A_n to produce a commitment of v_b. A_n outputs a bit b' and wins the game if $b' = b$.

Additionally, we consider commitment schemes that are "tag-based".

Definition 14 (Tag-based commitment scheme)**.** *A commitment scheme $\langle C, R\rangle$ is a tag-based scheme with $t(n)$-bit identities if, in addition to the security parameter 1^n, the committer and receiver also receive a "tag" – a.k.a. identity– $\mathsf{id} \in \{0,1\}^{t(n)}$ as common input.*

When the length $t(n)$ of identities is n, we refer to $\langle C, R\rangle$ as a tag-based commitment scheme. We say that a tag-based scheme with $t(n)$-bit identities is perfectly binding (resp., $\mathcal{C}$-hiding) if binding (resp., $\mathcal{C}$-hiding) holds for every $\mathsf{id} \in \{0,1\}^{t(n)}$.

Definition 15 (Over-extractable commitment scheme)**.** *A perfectly binding commitment scheme $\langle C, R\rangle$ is over-extractable w.r.t. extractor $o\mathcal{E} = \{o\mathcal{E}_n\}_{n\in\mathbb{N}}$ if for every polynomially bounded $\alpha(\cdot)$ and any $n \in \mathbb{N}$,*

$$\mathsf{Pr}\left[v' \leftarrow o\mathcal{E}_n(c) : c \text{ is valid } \wedge \mathsf{val}(c) \neq v'\right] = 0 \ , \tag{1}$$

where $n_c = n_c(n, \alpha(n))$ is the maximal length of the commitment generated by $\langle C, R\rangle$ with security parameter n and committing to $\alpha(n)$-bit values. Furthermore, we say $\langle C, R\rangle$ is (d, S)-over-extractable if the extractor $o\mathcal{E}$ belongs to the circuit class $\mathcal{C}^{\wedge}_{d,S}$.

Remark 3. *Note that the extractor $o\mathcal{E}$ must successfully (with probability 1) extract the correct value for any valid commitment (i.e., for which there exists a decommitment), even if the valid commitment is generated by a malicious committer.*

Remark 4. *In general, extractors $o\mathcal{E} = \{o\mathcal{E}_n\}_{n\in\mathbb{N}}$ (as in Definition 15) can be randomized and one can relax Equation 1 allowing extractors to fail with some negligible probability. As all extractors*

considered in this work are deterministic, we choose to state the stronger definition. We also note that our notion of (over)-extraction, commitment scheme differs from the notion of extractable commitments [Wee10] where the extractors can additionally interact with a malicious committer to extract the value of the commitment.

In the rest of the paper whenever we say a commitment scheme, we mean a perfectly binding commitment scheme.

THE MAN-IN-THE-MIDDLE (MIM) EXECUTION Let $\langle C, R\rangle$ be a tag-based commitment scheme. Consider a non-uniform circuit family $A = \{A_n\}_{n\in\mathbb{N}}$. For security parameter n and challenge bit $b \in \{0,1\}$ we refer to $\mathsf{MIM}^A_{\langle C,R\rangle}(1^n, b)$ as the man-in-the-middle execution where A_n participates in m-left and m-right concurrent interactions committing to values of length α.[11] We allow A_n complete control over scheduling of messages in all interactions. For every left interaction $i \in [m]$, A_n adaptively chooses a pair of values $(v_i^0, v_i^1) \in \{0,1\}^\alpha$ and an identity id_i at the start of this interaction, interacts with C to receive a commitment to the value v_i^b using the identity id_i. In right interactions A_n interacts with R attempting to commit to related values $\tilde{v}_1, \ldots, \tilde{v}_m$, using identities $\tilde{\mathsf{id}}_1, \tilde{\mathsf{id}}_2, \ldots, \tilde{\mathsf{id}}_m$ of its choice. We define the values $\tilde{v}_i$ committed on the right as $\tilde{v}_i = \mathsf{val}(\tilde{c}_i)$ where $\tilde{c}_i$ is the commitment in the ith right interaction. Recall that $\mathsf{val}(c) = \perp$, if c is not valid or that it can be opened to more than one value. Otherwise, $\mathsf{val}(c)$ equals the unique value v it can be opened to. Furthermore, if for any right interaction i, $\tilde{\mathsf{id}}_i = \mathsf{id}_j$ for some j, we set $\tilde{v}_i = \perp$.

We define two different flavours of non-malleability. First we recall the standard notion of non-malleability – a.k.a non-malleability w.r.t. commitment, for (tag-based) commitment schemes. Then, we introduce a new notion called non-malleability w.r.t. extraction for over-extractable commitment schemes.

Non-malleability w.r.t. commitment. Consider a MIM execution with A. For security parameter $n \in \mathbb{N}$ and bit $b \in \{0,1\}$, let $\mathsf{mim}^A_{\langle C,R\rangle}(1^n, b)$ denote the random variable that describes the values $\tilde{v}_1, \ldots, \tilde{v}_m$ that A commits to on the right and the view of A in $\mathsf{MIM}^A_{\langle C,R\rangle}(1^n, b)$ where view consists of the set of all messages A sends/receives in the MIM execution.

Definition 16 (Non-malleability)**.** *A tag-based commitment scheme $\langle C, R\rangle$ is said to be concurrent $\mathcal{C}$-non-malleable if for every circuit family $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ participating in $m = \mathsf{poly}(n)$ concurrent interactions, receiving/sending commitments to $\alpha = \mathsf{poly}(n)$-bit values, the following ensembles are computationally indistinguishable:*

$$\left\{\mathsf{mim}^A_{\langle C,R\rangle}(1^n, 0)\right\}_{n\in\mathbb{N}} \; ; \; \left\{\mathsf{mim}^A_{\langle C,R\rangle}(1^n, 1)\right\}_{n\in\mathbb{N}} .$$

Non-malleability w.r.t. extraction. Let $\langle C, R\rangle$ be a tag-based commitment scheme which is over-extractable w.r.t. extractor $o\mathcal{E}$. We say that $\langle C, R\rangle$ is non-malleable w.r.t. extraction if the distributions of the random variable emim defined below are indistinguishable. Recall that mim describes the view of A and the values $\tilde{v}_i$ that A commits to on the right. However, the random variable $\mathsf{emim}^A_{\langle C,R\rangle, o\mathcal{E}}(1^n, b)$[12], instead, describes the view of A and the values $\tilde{v}_i'$ which are obtained

[11] In standard definitions of non-malleability [DDN00, LPV08], the man-in-the-middle adversary is also given some auxiliary information z. In this work, we consider non-malleability against non-uniform circuits, which can be thought of as having z hard-wired in them. This is why we ignore z in our definitions.

[12] Note that in general the random variable emim should be parametrized by the extractor $o\mathcal{E}$. But in rest of this work we will drop it from the subscript for notational convenience as the underlying extractor will be clear from the context

by running the extractor $o\mathcal{E}$ on input $\tilde{c}_i$ (the ith right commitment); that is, $\tilde{v_i}' \leftarrow o\mathcal{E}_n(\tilde{c}_i)$. Note that, if for any right interaction i, $\tilde{\mathsf{id}}_i = \mathsf{id}_j$, for some j, then we set $\tilde{v_i}' = \perp$.

Definition 17 (Non-malleability w.r.t. extraction)**.** *A tag-based commitment scheme $\langle C, R\rangle$ is said to be concurrent $\mathcal{C}$-non-malleable w.r.t. extraction by $o\mathcal{E}$ if the following hold:*

1. *$\langle C, R\rangle$ is over-extractable by $o\mathcal{E}$.*
2. *For every circuit $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ participating in $m = \mathsf{poly}(n)$ concurrent interactions receiving/sending commitments to $\alpha = \mathsf{poly}(n)$-bit values, the following ensembles are computationally indistinguishable:*

$$\left\{\mathsf{emim}^{A}_{\langle C,R\rangle,o\mathcal{E}}(1^n, 0)\right\}_{n\in\mathbb{N}} \;;\; \left\{\mathsf{emim}^{A}_{\langle C,R\rangle,o\mathcal{E}}(1^n, 1)\right\}_{n\in\mathbb{N}} .$$

At first glance, it may seem that the new notion — non-malleability w.r.t. extraction, is no more interesting than the standard notion of non-malleability (w.r.t. commitment). After all, an extractor that agrees with the function val establishes that the two notions are equivalent. Most constructions of non-malleable commitment schemes in the literature, in fact, establish non-malleability by building such an extractor in their security proofs. In this work, however, we consider extractors that may not always agree with val and have some *over-extraction*.

Relationship between Non-malleability w.r.t. Commitment and w.r.t. Extraction. Over-extractability guarantees that for valid commitments, the extractor extracts out the committed value. However, given an invalid commitment, the value extracted by the extractor can be arbitrary. This inept behaviour of the extractor, on invalid commitments, is what makes the two notions incomparable (in general). For instance, there might exist an adversary A which depending on the value committed on the left may choose to send invalid transcripts on the right with different probabilities. Such an A certainly breaks the non-malleability of the scheme (w.r.t commitment) but depending on the extractor, A may not violate non-malleability w.r.t. extraction because the extracted values may still be indistinguishable. Furthermore, there might exist an adversary that irrespective of the value on the left always sends invalid commitments on the right. Such an A does not break the non-malleability w.r.t. commitment. But A may violate non-malleability w.r.t. extraction by establishing a co-relation between the value committed on the left and the value that will be over-extracted by the extractor on the right. Hence, the two notions are incomparable. However, if one sets up the decommitment condition (which defines the random variable mim) appropriately then we show that it is possible to base non-malleability w.r.t. commitment on non-malleability w.r.t. extraction. We believe this reduction as one of the main contributions of this work.

We also consider relaxed versions of both non-malleability and non-malleability w.r.t. extraction: one-one, one-many and many-one secure commitment schemes. In one-one (a.k.a. standalone), we consider an adversary A that participates in one left and one right interaction; in one-many A participates in one left and many right; and in many-one, A participates in many left and one right interaction.

Relationship between Non-malleability and Hiding. We note that any commitment scheme that is $\mathcal{C}$-non-malleable w.r.t. extraction (by extractor $o\mathcal{E}$) is also $\mathcal{C}$-hiding. This is because any adversary $A \in \mathcal{C}$ that breaks hiding (say w.r.t. $v_0, v_1 \in \{0,1\}^\alpha$) can send valid commitments to b^α on the right when receiving a commitment to v_b on the left. Then, due to the over-extraction of $o\mathcal{E}$,

A also breaks non-malleability w.r.t. extraction. In fact, this holds irrespective of the complexity of the extractor $o\mathcal{E}$ and also holds for the extractor that computes the function $\mathsf{val}(c)$ – the value of the commitment c.

Theorem 7. *Let $\langle C, R\rangle$ be a commitment scheme and $\mathcal{C}$ be a class of circuits that is closed under composition with $\mathcal{P}/\mathrm{poly}$.*

1. *If $\langle C, R\rangle$ is one-one $\mathcal{C}$-non-malleable w.r.t. commitment then it is $\mathcal{C}$-hiding.*
2. *If $\langle C, R\rangle$ is one-one $\mathcal{C}$-non-malleable w.r.t. extractor $o\mathcal{E}$ then it is $\mathcal{C}$-hiding (irrespective of the complexity of the extractor $o\mathcal{E}$).*

3.6 Time-Lock Puzzles

Definition 18 (Time-lock puzzles [BGJ+16])**.** *A (T, B)-time-lock (TL) puzzle is a tuple $(\mathsf{Gen}, \mathsf{Sol})$ satisfying the following requirements:*

1. *Syntax:*
   - *$Z \leftarrow \mathsf{Gen}(1^n, 1^t, s)$ is a probabilistic algorithm that takes as input a security parameter n, a solution $s \in \{0,1\}^n$ and a difficulty parameter t and outputs a puzzle Z.*
   - *$s \leftarrow \mathsf{Sol}(Z)$ is a deterministic algorithm that takes as input a puzzle Z and outputs a solution s.*
2. *Completeness: For every security parameter n, difficulty parameter t, solution $s \in \{0,1\}^n$ and puzzle Z in the support of $\mathsf{Gen}(1^n, 1^t, s)$, $\mathsf{Sol}(Z)$ outputs s.*
3. *Efficiency:*
   - *$Z \leftarrow \mathsf{Gen}(1^n, 1^t, s)$ is a poly-time algorithm, that is, it runs in time $\mathsf{poly}(t, n)$.*
   - *$s \leftarrow \mathsf{Sol}(Z)$ runs in time $\mathsf{poly}(2^t)$ for Z in the support of $\mathsf{Gen}(1^n, 1^t, \cdot)$.*
4. *(T, B)-hardness: $(\mathsf{Gen}, \mathsf{Sol})$ is a (T, B)-hard TL puzzle if for every $t(n) \in \omega(\log n) \cap n^{O(1)}$ and every adversary $A = \{A_n\}_{n\in\mathbb{N}}$ where,*

$$\mathsf{dep}(A_n) \leq T(t) \ ; \ \mathsf{size}(A_n) \leq B(n) \ ,$$

there exists a negligible function ν, such that for every $n \in \mathbb{N}$,

$$\Pr\left[s \leftarrow \{0,1\}^n; \ Z \leftarrow \mathsf{Gen}(1^n, 1^{t(n)}, s); \ s' \leftarrow A_n(Z) : s' = s\right] \leq \nu(n) \ .$$

The first candidate construction of TL puzzles was proposed by Rivest, Shamir and Wagner [RSW96] and is based on the "inherently sequential" nature of exponentiation modulo an RSA integer. Twenty years after their proposal, there still does not exist a (parallelizable) strategy that can solve the puzzle (of difficulty parameter t) in parallel-time $T(t)$ which is significantly less than 2^t. Apart from the variants of RSW puzzles [BN00, GMPY11], the only other construction of TL puzzles was given by Bitansky et al. [BGJ+16] based on succinct randomized encodings for Turing machines (which in turn can be built from indistinguishability obfuscation and one-way functions) and the existence of non-parallelizing languages. These previous works have considered puzzles with

strong parameters, that is, puzzles that are parallel-time hard for exponential $T = 2^{\delta t}$ ([BGJ+16]) and even strongly exponential $T = \delta 2^t$ ([BN00, GMPY11]).

However, for our task of constructing 2-round non-malleable commitments, much weaker TL puzzles are sufficient, that is, puzzles that remain hard for only subexponential $T = 2^{t^\delta}$ parallel-time. More precisely, we need a $(T(t) = 2^{t^\delta}, B(n) = 2^{n^\varepsilon})$-TL puzzle for some $0 < \varepsilon, \delta < 1$. We present the RSW TL puzzles $\mathsf{RSW} = (\mathsf{Gen}, \mathsf{Sol})$ as a candidate.

- Algorithm $\mathsf{Gen}(1^n, 1^t, s)$:

  1. Select an n-bit RSA modulous $N = pq$.
  2. Compute the mask $y = g^{2^{2^t}} \mod N$ for some element $g \in \mathbb{Z}_N^*$. Note that since the factorization of N is known, Gen can first compute the exponent $e = 2^{2^t} \mod \phi(N)$ and then efficiently compute the mask $y = g^e \mod N$.
  3. Mask the solution s with y, that is, $z = (s + y) \mod N$.
  4. Return the tuple $Z = (z, N)$ as the puzzle.

- Solver $\mathsf{Sol}(Z = (z, N))$:

  1. By 2^t repeated squarings, compute $y = g^{2^{2^t}} \mod N$.
  2. Output $(z - y) \mod N$ as the solution.

As discussed in [RSW96], the element g above can either be a fixed element such as 2, or sampled at random.

Next, we discuss that $\mathsf{RSW} = (\mathsf{Gen}, \mathsf{Sol})$ is a TL puzzle in the sense of Definition 18. It is easy to see that for security parameter n and difficulty parameter t, Gen runs in time $\mathsf{poly}(t, n)$ and Sol runs in time $\mathsf{poly}(2^t)$. Futhermore, we base the (T, B)-hardness of the RSW puzzle on the subexponential repeated squaring assumption as stated in Assumption 1. Informally, it says that for some subexponential functions T and B, and any function $t \in \omega(\log n) \cap n^{O(1)}$, $B(n)$-sized adversaries with depth $T(t)$ cannot compute $g^{2^{2^t}} \mod N$. We define the assumption more formally below.

Assumption 1 (Subexponential Repeated Squaring Assumption)**.** *There exists subexponential functions T, B such that for every function $t(\cdot) \in \omega(\log n) \cap n^{O(1)}$, the following holds: For every adversary $A = \{A_n\}_{n \in \mathbb{N}}$ such that*

$$\mathsf{dep}(A_n) \leq T(t(n)); \ \mathsf{size}(A_n) \leq B(n) \ ,$$

there exists a negligible function μ such that for every $n \in \mathbb{N}$, [13]

$$\Pr\left[N \leftarrow \mathsf{RSA}(n); \ g \leftarrow Z_N^*; \ y \leftarrow A_n(g, N) : y = g^{2^{2^t}} \mod N\right] \leq \mu(n) \ ,$$

where $\mathsf{RSA}(n)$ is the set of all n-bit RSA moduli.

Then, it is easy to see that if the subexponential repeated squaring assumption holds, then the RSW puzzle as defined above is a (T, B)-hard TL puzzle for some subexponential functions T and B.

Lemma 1. *If the subexponential repeated squaring assumption holds, then there exists subexponential functions T and B, such that, $\mathsf{RSW} = (\mathsf{Gen}, \mathsf{Sol})$ is a (T, B)-hard TL puzzle.*

[13] g can also be fixed appropriately instead of sampling it randomly.

3.7 Collision-resistant Hash Functions

Definition 19. *A family of $\mathcal{C}^{\wedge}_{S,S}$-collision-resistant hash functions (CRH) $\mathcal{H} = \{H_n\}_{n\in\mathbb{N}}$ is a function family ensemble such that for every $n \in \mathbb{N}$, $H_n = \{h : \{0,1\}^{m(n)} \to \{0,1\}^n\}$ such that $n < m(n)$ satisfying,*

1. *Efficient Sampling: There exists a poly-time TM S such that for every $n \in \mathbb{N}$, $S(1^n)$ outputs a uniform element of H_n.*
2. *Efficient Computation: There exists a poly-time TM M such that for every $n \in \mathbb{N}$, $h \in H_n$ and $x \in \{0,1\}^{m(n)}$, $M(h,x) = h(x)$.*
3. *$S(n)$-Collision-resistance: For every non-uniform circuit $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}^{\wedge}_{S,S}$ there exists a negligible function ν such that for every $n \in \mathbb{N}$,*

$$\mathsf{Pr}\left[h \leftarrow H_n, (x_1,x_2) \leftarrow A(h) : x_1 \neq x_2 \wedge h(x_1) = h(x_2)\right] \leq \nu(S(n)) \ . \tag{2}$$

We will sometimes refer to $\mathcal{C}^{\wedge}_{S,S}$-collision resistant hash family as S-collision resistant hash family. Moreover, a family of uniform *collision resistant hash function (CRH) is as defined above, except that i) the family H_n only consists of a single function h_n, and ii) $S(n)$-collision resistence only holds against attackers that are* $\mathsf{poly}(S(n))$*-time* uniform *Turing machines. We denote such a family as $\{h_n\}_{n\in\mathbb{N}}$.*

In this work, we will use subexp-secure, uniform or non-uniform, collision-resistant hash functions. For $n \in \mathbb{N}$ and any $h \in H_n$, a collision can be found by a uniform Turing machine in time $2^{n/2}$ with high probability and in time $\mathsf{poly}(n) \cdot 2^n$ with probability 1. Furthermore, for some $0 < \varepsilon < 1/2$, we require that it be hard for any $\mathsf{poly}(2^{n^\varepsilon})$-sized circuit (or a $\mathsf{poly}(2^{n^\varepsilon})$-time uniform Turing machine) to find collisons for a randomly chosen hash function $h \leftarrow H_n$ (or for h_n in the uniform case) for $0 < \varepsilon < 1/2$.

4 Basic Commitment Schemes

In this section we construct three basic over-extractable commitment schemes, each one of them enjoys hiding against different circuit classes. Firstly, we construct a depth-robust commitment scheme which is (S', S')-over-extractable and hiding against any circuit whose depth is sufficiently smaller than S'. Next, we construct a size-robust commitment scheme which is hiding against any circuit whose size is at most $\mathsf{poly}(S)$ but there exists an extractor of polynomial depth and size larger than S. Finally, we construct a commitment scheme which is hiding against both depth-restricted and size-restricted circuits.

4.1 Depth-robust Over-extractable Commitment Scheme from a TL-puzzle

For some subexponential functions T and B, assume the existence of a (T, B)-TL puzzle $(\mathsf{Gen}, \mathsf{Sol})$. For any difficulty parameter $t(n) \in \omega(\log n) \cap n^{O(1)}$, these puzzles are solvable in time $\mathsf{poly}(2^t)$ but hard for $B(n)$-sized circuits having depth at most $\mathsf{poly}(T(t))$.[14] Furthermore, consider a difficulty parameter $t(n)$ that admits the following hierarchy of non-decreasing functions, $n << d = T(t) <<$

[14]The definition of TL puzzles presented in Definition 18 defines hardness against circuits with depth at most T but for ease of description we assume hardness for $\mathsf{poly}(T)$ depth. This is without loss of generality for subexponential $T = 2^{t^{\delta'}}$, that is, hardness against $2^{t^{\delta'}}$ implies hardness against $\mathsf{poly}(2^{t^{\delta}})$ for any $\delta < \delta' < 1$.

$S' = 2^t << S^* << B$. Using the (T, B)-TL puzzles, we construct a commitment scheme which is over-extractable in time $\mathsf{poly}(S')$ and is hiding against any circuit in $\mathcal{C}_d$ (hence the name *depth-robust* commitment scheme). We refer to the commitment scheme as $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ which is described below. [15]

On input a security parameter 1^n, the honest committer C runs the algorithm ECom_d described below to commit to a value $v \in \{0,1\}^\alpha$. After the commit stage, the honest receiver R decides whether to accept the commitment by running the function EOpen_d as described in the reveal stage.

- Commit stage - Algorithm ECom_d:

  1. On input security parameter 1^n and value $v \in \{0,1\}^\alpha$, for every $0 \leq i \leq \alpha - 1$, ECom_d samples random strings $s_i, r_i \in \{0,1\}^n$ and computes the commitment c_i to $v[i]$, the ith bit of v, as follows,

  $$c_i = (Z_i = \mathsf{Gen}(1^n, 1^{t(n)}, s_i \; ; r), \; r_i, \; \langle r_i \cdot s_i \rangle \oplus v[i]) \; ,$$

  where r is the random tape used by Gen and t is the difficulty parameter such that $d = T(t)$.

  2. ECom_d sets the vector $c = \{c_i\}_{0 \leq i \leq \alpha - 1}$ as the commitment and sets $(v, \{s_i\}_{0 \leq i \leq \alpha - 1}, r)$ as the decommitment.

- Reveal stage - Function EOpen_d:
  On input commitment $c = \{c_i\}_{0 \leq i \leq \alpha - 1}$ and decommitment $(v, \{s_i\}_{0 \leq i \leq \alpha - 1}, r)$, EOpen_d returns 1 if $c_i = (\mathsf{Gen}(1^n, 1^t, s_i \; ; r), \; r_i, \; \langle r_i \cdot s_i \rangle \oplus v[i])$ for every $0 \leq i \leq \alpha - 1$. Otherwise, outputs 0.

Furthermore, the extractor $o\mathcal{E}_d$ of the scheme proceeds as follows:

- Extraction - Extractor $o\mathcal{E}_d$:
  On input any commitment $c = \{c_i = (Z_i, r_i, z_i)\}_{0 \leq i \leq \alpha - 1}$, the extractor $o\mathcal{E}_d$ computes the solution s_i of Z_i by running $\mathsf{Sol}(Z_i)$. Then, $o\mathcal{E}_d$ extracts bit $v[i]$ committed in c_i by computing $v[i] = z_i \oplus \langle r_i \cdot s_i \rangle$. $o\mathcal{E}_d$ returns the string $v[0] || \ldots || v[\alpha - 1]$ as its output.

Theorem 8. *Assume the existence of (T, B)-TL puzzles $(\mathsf{Gen}, \mathsf{Sol})$ for some subpexponential functions T and B. Then, for any $t(n) \in \omega(\log n) \cap n^{O(1)}$ and any non-decreasing function S^* satisfying $n << d = T(t) << S' = 2^t << S^* << B$, $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ is a non-interactive, perfectly binding, $\mathcal{C}_d$-hiding, (S', S')-over-extractable commitment scheme w.r.t. extractor $o\mathcal{E}_d$.*

Proof. We discuss each of the properties in the following:

- Efficiency: For any $n \in \mathbb{N}$, difficulty parameter $t = t(n)$ and length $\alpha = \alpha(n)$ which are upper-bounded by some polynomial, and $0 \leq i \leq \alpha - 1$, ECom_d runs Gen to sample puzzles Z_i's and rest of computation (i.e., sampling n-bit strings, computing inner-product) takes $\mathsf{poly}(n)$ time. In fact for difficulty parameter $t(n)$, Gen runs in time $\mathsf{poly}(t, n)$ which is upper-bounded by some $\mathsf{poly}(n)$ as t is upper-bounded by a polynomial. Hence, ECom_d runs in time $\mathsf{poly}(n)$ for each $0 \leq i \leq \alpha - 1$. Furthermore, since α is also upper-bounded by a polynomial, ECom_d is efficient.

[15] From now on, for notational convenience, we represent a non-interactive commitment scheme by the tuple of commit and open algorithms; that is $(\mathsf{ECom}, \mathsf{EOpen})$, instead of a pair of interactive TMs C and R.

- Perfect binding: Note that TL-puzzles are injective, that is, any (even arbitrarily generated) Z belongs to the support of $\mathsf{Gen}(1^n, 1^t, s)$ for at most one solution $s \in \{0,1\}^n$. Assume towards a contradiction that there exists a Z that belongs to the support of both $\mathsf{Gen}(1^n, 1^t, s_0)$ and $\mathsf{Gen}(1^n, 1^t, s_1)$ for some $s_0 \neq s_1$. Let $s = \mathsf{Sol}(Z)$ be the output of the deterministic algorithm Sol on input Z. If $s \neq s_0$ then this contradicts the completeness of Sol w.r.t. puzzles in the support of $\mathsf{Gen}(1^n, 1^t, s_0)$. If $s = s_0$ then it contradicts the completeness of Sol w.r.t. puzzles in the support of $\mathsf{Gen}(1^n, 1^t, s_1)$. Therefore, for any puzzle Z there exists at most one solution s and in the case when a solution s exists we know $s = \mathsf{Sol}(Z)$.[16]

  Now, let $c = \{c_i = (Z_i, r_i, z_i)\}_{0 \leq i \leq \alpha(n)-1}$ be any commitment. From the above observation, we know that every Z_i falls in the support of at most one s_i. Therefore, for c there exists at most one sequence $(v, \{s_i\}_{0 \leq i \leq \alpha(n)-1})$ for which EOpen_d returns 1. This implies perfect binding of $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$.

- Over-extractable: First, the extractor $o\mathcal{E}_d$ belongs to the class $\mathcal{C}^{\wedge}_{S',S'}$ since Sol runs in time $\mathsf{poly}(S') = \mathsf{poly}(2^t)$ and the rest of the computation takes $\mathsf{poly}(n)$ time.

  Note that for any valid commitment $c = \{c_i = (Z_i, r_i, z_i)\}_{0 \leq i \leq \alpha(n)-1}$, Z_i's are honestly generated puzzles and furthermore each Z_i belongs to the support of $\mathsf{Gen}(1^n, 1^t, s_i)$ for exactly one s_i. These s_i's along with the r_i's (from c) uniquely define $\mathsf{val}(c)$, the value of the commitment. Moreover given (s_i, r_i)'s $\mathsf{val}(c)$ is efficiently computable.

  Then on any valid commitment c as input, the extractor $o\mathcal{E}_d$ first runs Sol on each of the Z_i's. Due to the perfect correctness of Sol, the extractor $o\mathcal{E}_d$ always extracts the corresponding s_i's and hence also the correct unique committed value, $\mathsf{val}(c)$. Therefore, $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ is (S', S')-over-extractable.

- Hiding: Let $t(n) = \omega(\log n)$ be some polynomially bounded difficulty parameter. Then by the definition of (T, B)-hardness of the TL puzzle we know that any adversary $A = \{A_n\}_{n \in \mathbb{N}}$, with $\mathsf{dep}(A_n) \leq \mathsf{poly}(T(t))$ and $\mathsf{size}(A_n) \leq \mathsf{poly}(S^*) < B$, solves the puzzle $Z \leftarrow \mathsf{Gen}(1^n, 1^t, s)$ only with negligible probability for some randomly chosen s. Therefore, the distribution

$$\{s \leftarrow \{0,1\}^n,\ Z \leftarrow \mathsf{Gen}(1^n, 1^t, s)\ :\ (s, Z)\}\ , \tag{3}$$

  is unpredictable for any such adversary A. In our construction of $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$, we sample the TL puzzles with difficulty t such that $T(t) = d$. Therefore, the above distribution is $\mathcal{C}_d$-unpredictable. Then, by a standard argument (see Theorem 4) about the hardcoreness of the Goldreich Levin bit [GL89] extracted from an $\mathcal{C}_d$-unpredictable distribution, we can conclude that the function that on input (s, r) outputs $\langle s \cdot r \rangle$ is hardcore for circuits in the class $\mathcal{C}_d$.[17] This then implies that $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ is $\mathcal{C}_d$-hiding.

□

4.2 Size-robust Over-extractable Commitment Scheme from Injective OWFs

For a non-decreasing function $S(n)$ ($<< S^*(n)$), assume that there exists an injective one-way function (OWF) f that is hard to invert for any $\mathsf{poly}(S)$-sized circuit (for any polynomial $\mathsf{poly}(\cdot)$),

[16] It can be possible that some Z does not belong to the support of any $\mathsf{Gen}(1^n, 1^t, s)$ for any s, in which case we say that Z has no solution.

[17] Here we rely crucially on the fact that the GL reduction only blows up the depth of the adversary by a polynomial factor (Remark 2). Therefore, allowing us to base the $\mathcal{C}_d$-hardcoreness of the GL-bit $\langle s \cdot r \rangle$ on the $\mathcal{C}_d$-hardness of the TL puzzles.

but there exists a non-decreasing function $S''(n)$ ($S << S'' << S^*$) such that a circuit of $\mathsf{poly}(n)$ depth and S'' size can invert it. Such an injective OWF can be instantiated from a subexponentially secure injective OWF by setting the input length k appropriately. More concretely, consider a subexponentially secure injective OWF that is hard for circuits of size $\mathsf{poly}(2^{k^\varepsilon})$ (for any polynomial $\mathsf{poly}()$ and some $0 < \varepsilon < 1$). For any S, we can design the required f which is hard to invert for $\mathsf{poly}(S)$-sized circuits by setting $k = (\log S)^{1/\varepsilon}$, thereby achieving security against circuits of size $\mathsf{poly}(2^{k^\varepsilon}) = \mathsf{poly}(2^{(\log S)})$. Furthermore, there exists a circuit which can invert (with probability 1) by enumerating all the 2^k pre-images. Such a circuit has size $S'' = \mathsf{poly}(2^k) = \mathsf{poly}(2^{(\log S)^{1/\varepsilon}}) >> S$ and polynomial depth.

Using such an injective OWF f, we construct $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ – a commitment scheme which is hiding against circuits of size $\mathsf{poly}(S)$ (hence the name *size-robust* commitment scheme) and $(\mathsf{poly}(n), S'')$-over-extractable. $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ is simply the non-interactive commitment scheme based on injective OWFs where the hard-core predicate is the Golreich-Levin bit [GL89]. For completeness, we describe the scheme below.

As before, on input a security parameter 1^n, the honest committer C runs the algorithm ECom_S described below to commit to a value $v \in \{0,1\}^\alpha$. After the commit stage, the honest receiver R decides whether to accept the commitment by running the function EOpen_S as described in the reveal stage.

- Commit stage - Algorithm ECom_S:

  1. On input security parameter 1^n and value $v \in \{0,1\}^\alpha$, for every $0 \leq i \leq \alpha - 1$, ECom_S samples random strings s_i in the domain of f, random strings $r_i \leftarrow\!\!\$\, \{0,1\}^{|s_i|}$ and computes the commitment c_i to $v[i]$, the ith bit of v, as follows,

  $$c_i = (f(s_i),\ r_i, \langle r_i \cdot s_i \rangle \oplus v[i])\ .$$

  2. ECom_S sets the vector $c = \{c_i\}_{0 \leq i \leq \alpha-1}$ as the commitment and sets $(v, \{s_i\}_{0 \leq i \leq \alpha-1})$ as the decommitment.

- Reveal stage - Function EOpen_S:
  On input commitment $c = \{c_i\}_{0 \leq i \leq \alpha-1}$ and decommitment $(v, \{s_i\}_{0 \leq i \leq \alpha-1})$, EOpen_S returns 1 if $c_i = (f(s_i),\ r_i,\ \langle r_i \cdot s_i \rangle \oplus v[i])$ for every $0 \leq i \leq \alpha - 1$. Otherwise, outputs 0.

The extractor $o\mathcal{E}_S$ for the scheme proceeds as follows:

- Extraction - Extractor $o\mathcal{E}_S$:
  On input any commitment $c = \{c_i = (y_i, r_i, z_i)\}_{0 \leq i \leq \alpha-1}$, the extractor $o\mathcal{E}_S$ computes the pre-image s_i of y_i under f (by assumption, f can be inverted using a circuit of polynomial depth and S'' size). $o\mathcal{E}_S$ extracts bit $v[i]$ committed in c_i by computing $v[i] = z_i \oplus \langle r_i \cdot s_i \rangle$. $o\mathcal{E}_S$ returns the string $v[0]||\ldots||v[\alpha-1]$ as its output.

Theorem 9. *If f is a $\mathcal{C}^\wedge_{S,S}$-secure injective OWF which is invertible by a circuit in $\mathcal{C}^\wedge_{\mathsf{poly}(n),S''}$ for non-decreasing functions S, S'' such that $n << S << S'' << S^*$ then $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ is a non-interactive, perfectly binding, $\mathcal{C}^\wedge_{S,S}$-hiding and $(\mathsf{poly}(n), S'')$-over-extractable commitment scheme w.r.t. extractor $o\mathcal{E}_S$.*

Proof. We discuss all the properties in the following:

- Binding and Hiding: The proof of perfect binding follows from the injectivity of f and proof of $\mathcal{C}^{\wedge}_{S,S}$-hiding follows from the hard-coreness of the Goldreich-Levin bit with f being $\mathcal{C}^{\wedge}_{S,S}$ one-way (hence the scheme is $\mathcal{C}^{\wedge}_{S,S}$-hiding).

- Over-extractable: First, the extractor $o\mathcal{E}_S$ belongs to the class $\mathcal{C}^{\wedge}_{\mathsf{poly}(n),S''}$ since f can be inverted by a circuit in $\mathcal{C}^{\wedge}_{\mathsf{poly}(n),S''}$ and the rest of the computation takes $\mathsf{poly}(n)$ time. Furthermore, since $o\mathcal{E}_S$ always inverts OWF images y_i's correctly, it always extracts the correct unique committed value. Therefore, $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ is $(\mathsf{poly}(n), S'')$-over-extractable.

□

4.3 Strong Over-extractable Commitment Scheme

For non-decreasing functions,

$$n << d(n) << S'(n), S(n) << S''(n) << S^*(n) << 2^{n^\varepsilon} ,$$

we construct a non-interactive perfectly binding commitment $(\mathsf{ECom}_{d,S}, \mathsf{EOpen}_{d,S})$ which is $\mathcal{C}^{\vee}_{d,S}$-hiding and (S', S'')-over-extractable w.r.t an extractor $o\mathcal{E}_{d,S}$. Note that, unlike the commitment schemes described in Sections 4.1 and 4.2 which were either hiding against depth-restricted circuits $\mathcal{C}_d$ or hiding against size-restricted circuits $\mathcal{C}^{\wedge}_{S,S}$, $(\mathsf{ECom}_{d,S}, \mathsf{EOpen}_{d,S})$ enjoys a *stronger* security property of being hiding against circuits in both depth-restricted and size-restricted circuit classes (i.e., $\mathcal{C}^{\vee}_{d,S}$). We describe the construction of the scheme $(\mathsf{ECom}_{d,S}, \mathsf{EOpen}_{d,S})$ for an honest committer C and an honest receiver R below. The idea is to commit to a random 2-out-of-2 secret share of the value v using each of the schemes described in Sections 4.1 and 4.2.

As before, on input a security parameter 1^n, the honest committer C runs the algorithm $\mathsf{ECom}_{d,S}$ described below to commit to a value $v \in \{0,1\}^\alpha$. After the commit stage, the honest receiver R decides whether to accept the commitment by running the function $\mathsf{EOpen}_{d,S}$ as described in the reveal stage.

- Commit stage - Algorithm $\mathsf{ECom}_{d,S}$:

  1. On input security parameter 1^n and value $v \in \{0,1\}^\alpha$, $\mathsf{ECom}_{d,S}$ samples a random α-bit string r_0.
  2. $\mathsf{ECom}_{d,S}$ computes a commitment c_1 to r_0 using ECom_d. Let d_1 be the corresponding decommitment string.
  3. $\mathsf{ECom}_{d,S}$ computes a commitment c_2 to $v \oplus r_0$ using ECom_S. Let d_2 be the corresponding decommitment string.
  4. $\mathsf{ECom}_{d,S}$ sets (c_1, c_2) as the commitment c and sets (v, r_0, d_1, d_2) as the decommitment.

- Reveal stage - Function $\mathsf{EOpen}_{d,S}$:
  On input a commitment $c = (c_1, c_2)$ and the decommitment (v, r_0, d_1, d_2), $\mathsf{EOpen}_{d,S}$ accepts it if both EOpen_d and EOpen_S accept the corresponding decommitments; that is,

  $$\mathsf{EOpen}_d(c_1, r_0, d_1) = 1 \wedge \mathsf{EOpen}_S(c_2, v \oplus r_0, d_2) = 1 .$$

  Otherwise, $\mathsf{EOpen}_{d,S}$ rejects.

The extractor $o\mathcal{E}_{d,S}$ of the scheme proceeds as follows:

- Extraction - Extractor $o\mathcal{E}_{d,S}$:
The extractor $o\mathcal{E}_{d,S}$ on input $c = (c_1, c_2)$ runs the extractors $o\mathcal{E}_d$ and $o\mathcal{E}_S$ with inputs c_1 and c_2, obtaining outputs r'_0 and r'_1 respectively. If either r'_0 or r'_1 is $\perp$ then $o\mathcal{E}_{d,S}$ outputs $\perp$. Otherwise, $o\mathcal{E}_{d,S}$ outputs $r'_0 \oplus r'_1$.

Theorem 10. *For the following hierarchy of non-decreasing functions on* $\mathbb{N}$

$$n << d << S' << S << S'' << S^* << B \ ,$$

let $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ *be a non-interactive, perfectly binding,* $\mathcal{C}_d$*-hiding and* (S', S')*-over-extractable commitment scheme w.r.t. extractor* $o\mathcal{E}_d$ *and let* $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ *be a non-interactive, perfectly binding,* $\mathcal{C}^{\wedge}_{S,S}$*-hiding and* $(\mathsf{poly}(n), S'')$*-over-extractable commitment scheme w.r.t. extractor* $o\mathcal{E}_S$*. Then,* $(\mathsf{ECom}_{d,S}, \mathsf{EOpen}_{d,S})$ *is non-interactive, perfectly binding,* $\mathcal{C}^{\vee}_{d,S}$*-hiding and* (S', S'')*-over-extractable commitment scheme w.r.t. extractor* $o\mathcal{E}_{d,S}$*.*

Remark 5. *For our final construction of concurrent non-malleable commitment, we require the existence of* $(\mathsf{ECom}_d, \mathsf{EOpen}_d)$ *and* $(\mathsf{ECom}_S, \mathsf{EOpen}_S)$ *for some specific functions* d, S', S, S''*. Such schemes can be based on the existence of subexponentially secure injective OWFs and* (T, B)*-TL puzzles for some subexponential functions* T, B*. We provide concrete instantiations of such depth- and size-robust schemes in Section 8.2.*

Proof. We discuss each of the properties in the following:

- Perfect binding: The perfect binding follows from the perfect binding of ECom_d and ECom_S.

- Over-extractable: A valid commitment $c = (c_1, c_2)$ is such that both c_1 and c_2 are valid commitments for ECom_d and ECom_S respectively. Since ECom_d and ECom_S are over-extractable w.r.t. extractors $o\mathcal{E}_d$ and $o\mathcal{E}_S$ respectively, $o\mathcal{E}_{d,S}$ which runs $o\mathcal{E}_d(c_1)$ and $o\mathcal{E}_S(c_2)$ extracts out the unique committed values and hence outputs $\mathsf{val}(c)$ with probability 1. Furthermore, $o\mathcal{E}_d \in \mathcal{C}^{\wedge}_{S',S'}$ and $o\mathcal{E}_S \in \mathcal{C}^{\wedge}_{\mathsf{poly}(n),S''}$ implies that $o\mathcal{E}_{d,S}$ belongs to the circuit class $\mathcal{C}^{\wedge}_{S',S''}$.

- Hiding: Assume towards a contradiction that there exists a polynomially bounded function $\alpha(\cdot)$, a non-uniform circuit family $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}^{\vee}_{d,S}$ and for some polynomial $p(\cdot)$ and infinitely many $n \in \mathbb{N}$, a pair of values $v_0, v_1 \in \{0,1\}^{\alpha}$,

$$\mathsf{Pr}\left[b \leftarrow \{0,1\}, c \leftarrow \mathsf{ECom}_{d,S}(1^n, v_b) : b = A_n(c)\right] \geq \frac{1}{2} + \frac{1}{p(n)} \ . \tag{4}$$

  Using A, we construct a non-uniform circuit family $B = \{B_n\}_{n\in\mathbb{N}}$ that breaks the hiding of either ECom_d or ECom_S depending on the depth and size of A. Since $A \in \mathcal{C}^{\vee}_{d,S}$, it could either be that $A \in \mathcal{C}_d$ or $A \in \mathcal{C}^{\wedge}_{S,S}$. We will consider the two cases separately below.

  Case 1 - $A \in \mathcal{C}^{\wedge}_{S,S}$: In this case, we construct a B that violates the hiding of ECom_S as follows: B_n with v_0 and v_1 hard-wired in it, samples a random $\alpha(n)$-bit string r_0 and computes a commitment c_1 to string r_0 using ECom_d. It sends $(v_0 \oplus r_0)$ and $(v_1 \oplus r_0)$ as challenges in the hiding game of ECom_S and receives a commitment c_2 to $(v_b \oplus r_0)$, for a randomly chosen bit b. Finally, B_n sends the tuple (c_1, c_2) as the commitment to A_n and forwards the output of A_n as its output. B perfectly simulates the hiding game of $\mathsf{ECom}_{d,S}$ for A while itself participating in the hiding game of ECom_S and hence succeeds with probability at least $\frac{1}{2} + \frac{1}{p(n)}$. Furthermore, since B incurs only polynomial blow-up in size over A (while

simulating the game for A), we have $B \in \mathcal{C}^{\wedge}_{S,S}$. Therefore, $B \in \mathcal{C}^{\wedge}_{S,S}$ succeeds in the hiding game of ECom_S with non-negligible probability away from $\frac{1}{2}$, which is a contradiction.

Case 2 - $A \in \mathcal{C}_d$: The proof for Case 2 is similar to Case 1 but here we, instead, construct $B \in \mathcal{C}_d$ which succeeds in the hiding game of ECom_d with non-negligible probability away from $\frac{1}{2}$. The only difference from the previous case is that B commits to r_0 using the scheme ECom_S and forwards $(v_0 \oplus r_0)$ and $(v_1 \oplus r_0)$ as challenges in the hiding game of ECom_d. Since the marginal distribution of both random shares of v (i.e., r and $v \oplus r$ for a random r) are identical, B still perfectly simulates the hiding game of $\mathsf{ECom}_{d,S}$ for A.

□

5 Non-malleable Commitment Scheme w.r.t. Extraction for Short Identities

For $l = O(1)$ which is a power of 2, assume that we have the following hierarchy of non-decreasing functions on $\mathbb{N}$,

$$\begin{aligned} n << d_0 << d_1 << \ldots << d_{l-1} << d_l << \\ S_0 << S_1 << \ldots << S_{l-1} << S_l << S^* << 2^{n^\varepsilon} \ , \end{aligned} \tag{5}$$

such that for every $0 \leq \mathsf{id} \leq l-1$,

- there exists a depth-robust commitment scheme $(\mathsf{ECom}_{d_{\mathsf{id}}}, \mathsf{EOpen}_{d_{\mathsf{id}}})$ that is $\mathcal{C}_{d_{\mathsf{id}}}$-hiding and $(d_{\mathsf{id}+1}, d_{\mathsf{id}+1})$-over-extractable w.r.t. an extractor $o\mathcal{E}_{d_{\mathsf{id}}}$.
- there exists a size-robust commitment scheme $(\mathsf{ECom}_{S_{\mathsf{id}}}, \mathsf{EOpen}_{S_{\mathsf{id}}})$ that is $\mathcal{C}^{\wedge}_{S_{\mathsf{id}},S_{\mathsf{id}}}$-hiding and $(\mathsf{poly}(n), S_{\mathsf{id}+1})$-over-extractable w.r.t. an extractor $o\mathcal{E}_{S_{\mathsf{id}}}$.

By Section 4.3, we can construct a family of l commitments $\{(\mathsf{ECom}_{\mathsf{id}}, \mathsf{EOpen}_{\mathsf{id}})\}_{\mathsf{id}}$ such that for every $0 \leq \mathsf{id} \leq l-1$,

$$(\mathsf{ECom}_{\mathsf{id}}, \mathsf{EOpen}_{\mathsf{id}}) = (\mathsf{ECom}_{d_{\mathsf{id}},S_{l-\mathsf{id}-1}}, \mathsf{EOpen}_{d_{\mathsf{id}},S_{l-\mathsf{id}-1}}) \ ,$$

and by Theorem 10 we have that $(\mathsf{ECom}_{\mathsf{id}}, \mathsf{EOpen}_{\mathsf{id}})$ is a non-interactive, perfectly binding, $\mathcal{C}^{\vee}_{d_{\mathsf{id}},S_{l-\mathsf{id}-1}}$-hiding and also $(d_{\mathsf{id}+1}, S_{l-\mathsf{id}})$-over-extractable commitment scheme w.r.t. an extractor $o\mathcal{E}_{\mathsf{id}}$ (described in Section 4.3). We use this family of l commitment schemes to construct a tag-based commitment scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ for identities of length $\log l$-bits which is one-one non-malleable w.r.t. extraction by an extractor $o\mathcal{E}_{\mathsf{NM}}$. We describe the scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ and the extractor $o\mathcal{E}_{\mathsf{NM}}$ below.

On input a security parameter 1^n, the honest committer C runs the algorithm ENMCom described below to commit to a value $v \in \{0,1\}^\alpha$. After the commit stage, the honest receiver R decides whether to accept the commitment by running the function $\mathsf{ENMOpen}$ as described in the reveal stage.

- Commit stage - Algorithm ENMCom:

  1. On input security parameter 1^n, identity $0 \leq \mathsf{id} \leq l-1$ and a value $v \in \{0,1\}^\alpha$, ENMCom computes a commitment c to v using $\mathsf{ECom}_{\mathsf{id}}$. Let d be the corresponding decommitment string.

- Reveal stage - Function $\mathsf{ENMOpen}$:
  On input a commitment c and the decommitment (v, d) and identity id, $\mathsf{ENMOpen}$ computes $\mathsf{ENMOpen}(\mathsf{id}, c, v, d)$ which returns 1 if $\mathsf{EOpen}_{\mathsf{id}}(c, v, d)$ returns 1. Otherwise, returns 0.

The extractor $o\mathcal{E}_{\mathsf{NM}}$ proceeds as follows,

- Extraction - Extractor $o\mathcal{E}_{\mathsf{NM}}$:
  The extractor $o\mathcal{E}_{\mathsf{NM}}$ on input c and identity id outputs the value extracted by $o\mathcal{E}_{\mathsf{id}}$ from c.

Remark 6. *We want* ENMCom *and* $\mathsf{ENMOpen}$ *to be computable by uniform TMs. This mandates that* $\{\mathsf{ECom}_{\mathsf{id}}\}_{0\leq\mathsf{id}\leq l-1}$ *and* $\{\mathsf{EOpen}_{\mathsf{id}}\}_{0\leq\mathsf{id}\leq l-1}$ *be uniformly and efficiently computable; that is, there must exist uniform* PPT *TMs* M_{com} *and* M_{open} *that on input* id *can compute* $\mathsf{ECom}_{\mathsf{id}}$ *and* $\mathsf{EOpen}_{\mathsf{id}}$ *respectively. If* $l = O(1)$ *then one can simply hard-code all the algorithms* $\{\mathsf{ECom}_{\mathsf{id}}\}_{0\leq\mathsf{id}\leq l-1}$ *and* $\{\mathsf{EOpen}_{\mathsf{id}}\}_{0\leq\mathsf{id}\leq l-1}$ *in* M_{com} *and* M_{open} *respectively. As will see later,* $l = O(1)$ *is sufficient for constructing non-malleable commitment scheme for* n*-bit identities. When* $l = \omega(1)$ *the hard-coding approach, in fact, does not work. Nevertheless, we note that the algorithms* $\mathsf{ECom}_{\mathsf{id}}$ *and* $\mathsf{EOpen}_{\mathsf{id}}$ *described in Section 4.3 are still efficiently and uniformly computable. Since, this case does not occur in our construction, we omit details here.*

Theorem 11. $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ *is a non-interactive, perfectly binding,* $\mathcal{C}^{\wedge}_{d_0,S_0}$*-hiding and* (d_l, S_l)*-over-extractable tag-based commitment scheme for identities of length* $\log l$*.* $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ *is also one-one* $\mathcal{C}^{\wedge}_{d_0,S_0}$*-non-malleable w.r.t. extraction by extractor* $o\mathcal{E}_{\mathsf{NM}}$*.*

We note that both hiding and non-malleability hold only against circuits in the restrictive class $\mathcal{C}^{\wedge}_{d_0,S_0}$; that is, circuits A whose depth and size are bounded by $\mathsf{poly}(d_0)$ and $\mathsf{poly}(S_0)$ respectively, even though the building blocks $\mathsf{ECom}_{\mathsf{id}}$'s have the stronger security of being hiding against circuits in $\mathcal{C}^{\vee}_{d_{\mathsf{id}},S_{l-\mathsf{id}-1}} \supset \mathcal{C}^{\wedge}_{d_0,S_0}$; that is, circuits A which are either restricted in their depths or their size but not both.

Proof. The perfect binding follows readily from the perfect binding of each of the $\mathsf{ECom}_{\mathsf{id}}$'s. We discuss over-extractability and non-malleability in the following:

- Over-extractable: A valid commitment c with identity id is a valid commitment for $\mathsf{ECom}_{\mathsf{id}}$. Therefore, the extractor $o\mathcal{E}_{\mathsf{NM}}$ which runs $o\mathcal{E}_{\mathsf{id}}$ on c extracts the correct unique committed value due to the over-extractability of $\mathsf{ECom}_{\mathsf{id}}$ w.r.t. $o\mathcal{E}_{\mathsf{id}}$. Furthermore, $\mathsf{ECom}_{\mathsf{id}}$'s are $(d_{\mathsf{id}+1}, S_{l-\mathsf{id}})$-over-extractable and hence the depth of $o\mathcal{E}_{\mathsf{id}}$ is at most $\mathsf{poly}(d_{\mathsf{id}+1})$ and size of $o\mathcal{E}_{\mathsf{id}}$ is at most $\mathsf{poly}(S_{l-\mathsf{id}})$. Therefore, $o\mathcal{E}_{\mathsf{NM}}$ (which runs $o\mathcal{E}_{\mathsf{id}}$) is a circuit with depth bounded by $\mathsf{poly}(d_l)$ and size bounded by $\mathsf{poly}(S_l)$ (see Inequality (5)). Hence, $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ is (d_l, S_l)-over-extractable.

- Non-malleability and Hiding: By Theorem 7 hiding will follow from the proof of non-malleability which we describe next. For proving one-one non-malleability w.r.t. extraction by $o\mathcal{E}_{\mathsf{NM}}$, let us assume for contradiction that there exists a non-uniform attacker $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}^{\wedge}_{d_0,S_0}$ sending/receiving commitments to values of length $\alpha = \mathsf{poly}(n)$, a non-uniform distinguisher $D = \{D_n\}_{n\in\mathbb{N}} \in \mathcal{P}/\mathrm{poly}$, and a polynomial $p(\cdot)$, such that, for infinitely many $n \in \mathbb{N}$,

$$\left|\mathsf{Pr}[D_n(\mathsf{emim}^{A_n}_{\mathsf{ENMCom}}(1^n, 0)) = 1] - \mathsf{Pr}[D_n(\mathsf{emim}^{A_n}_{\mathsf{ENMCom}}(1^n, 1)) = 1]\right| \geq 1/p(n). \tag{6}$$

  Let id and $\tilde{\mathsf{id}}$ be the identities chosen by A in the left and right interactions respectively. Let $v_0, v_1 \in \{0,1\}^{\alpha}$ be the two challenge values chosen by A for the left interaction. Note that

since the only message A receives in the execution is the left commitment and identity and the values for the left interaction needs to be chosen before that, we can assume that the left side identity id and the challenge values v_0, v_1 are fixed.

Using A and D, we will construct a non-uniform circuit $B = \{B_n\}_{n\in\mathbb{N}} \in \mathcal{C}^{\vee}_{d_{\mathsf{id}}, S_{l-\mathsf{id}-1}}$ that breaks the hiding of $\mathsf{ECom}_{\mathsf{id}}$ with advantage at least $\frac{1}{p(n)}$. More concretely, B internally runs A and acts as an honest committer in the left interaction with A while acts as an honest receiver in the right interaction. In the hiding game of $\mathsf{ECom}_{\mathsf{id}}$, B sends (v_0, v_1) as challenges and receives a commitment c to v_b, for a randomly chosen bit b. B forwards c to A as the commitment in the left interaction. A sends a commitment $\tilde{c}$ to the honest right receiver (simulated by B). Then, B runs the extractor $o\mathcal{E}_{\tilde{\mathsf{id}}}$ on $\tilde{c}$ obtaining an extracted value $\tilde{v}'$. Depending on the value of b, the over-extracted value $\tilde{v}'$ along with the view of A is identical to $\mathsf{emim}^{A}_{\mathsf{ENMCom}}(1^n, b)$. B runs the distinguisher D with inputs $\tilde{v}'$ and the view of A. Finally, B returns the output of D as its output.

By our hypothesis, B succeeds in breaking the hiding of $\mathsf{ECom}_{\mathsf{id}}$ with advantage at least $\frac{1}{p(n)}$. Now to arrive at a contradiction it remains to show that $B \in \mathcal{C}^{\vee}_{d_{\mathsf{id}}, S_{l-\mathsf{id}-1}}$. B runs the extractor $o\mathcal{E}_{\tilde{\mathsf{id}}} \in \mathcal{C}^{\wedge}_{d_{\tilde{\mathsf{id}}+1}, S_{l-\tilde{\mathsf{id}}}}$ and $A \in \mathcal{C}^{\wedge}_{d_0, S_0}$, while the rest of the simulation takes $\mathsf{poly}(n)$ time. Therefore the depth of B is such that,

$$\begin{aligned} \mathsf{dep}(B) &= \mathsf{dep}(A) + \mathsf{dep}(o\mathcal{E}_{\tilde{\mathsf{id}}}) + \mathsf{poly}(n) \\ &\leq \mathsf{poly}(d_0) + \mathsf{poly}(d_{\tilde{\mathsf{id}}+1}) + \mathsf{poly}(n) < \mathsf{poly}(d_{\tilde{\mathsf{id}}+1}) \ . \end{aligned} \tag{7}$$

Similarly, the size of B is such that,

$$\begin{aligned} \mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{size}(o\mathcal{E}_{\tilde{\mathsf{id}}}) + \mathsf{poly}(n) \\ &\leq \mathsf{poly}(S_0) + \mathsf{poly}(S_{l-\tilde{\mathsf{id}}}) + \mathsf{poly}(n) \\ &< \mathsf{poly}(S_{l-\tilde{\mathsf{id}}}) << S^* \ . \end{aligned} \tag{8}$$

We consider two cases for the identities id and $\tilde{\mathsf{id}}$ as follows:[18]

Case 1 - $\mathsf{id} > \tilde{\mathsf{id}}$: In this case, $d_{\mathsf{id}} \geq d_{\tilde{\mathsf{id}}+1}$, we have that $\mathsf{dep}(B) < \mathsf{poly}(d_{\mathsf{id}})$ for some polynomial $\mathsf{poly}(\cdot)$. Therefore, $B \in \mathcal{C}_{d_{\mathsf{id}}}$ and hence $B \in \mathcal{C}^{\vee}_{d_{\mathsf{id}}, S_{l-\mathsf{id}-1}}$.

Case 2 - $\mathsf{id} < \tilde{\mathsf{id}}$: In this case, $S_{l-\tilde{\mathsf{id}}} \leq S_{l-\mathsf{id}-1}$ and we have that $\mathsf{size}(B) < \mathsf{poly}(S_{l-\mathsf{id}-1})$ for some polynomial $\mathsf{poly}(\cdot)$. Therefore $B \in \mathcal{C}^{\vee}_{d_{\mathsf{id}}, S_{l-\mathsf{id}-1}}$.

Thus, irrespective of the identity $\tilde{\mathsf{id}}$ chosen by A for the right interaction, we can construct $B \in \mathcal{C}^{\vee}_{d_{\mathsf{id}}, S_{l-\mathsf{id}-1}}$ which breaks hiding of $\mathsf{ECom}_{\mathsf{id}}$ with non-negligible advantage, which is a contradiction.

□

Remark 7. *In the above proof, the reduction B which bases the one-one non-malleability w.r.t. extraction on the hiding of $\mathsf{ECom}_{\mathsf{id}}$, runs both A and the extractor $o\mathcal{E}_{\tilde{\mathsf{id}}}$ of the commitment scheme $\mathsf{ECom}_{\tilde{\mathsf{id}}}$. Therefore, B has depth at most $\mathsf{dep}(A) + \mathsf{poly}(d_{\tilde{\mathsf{id}}+1})$ and has size at most $\mathsf{size}(A) + \mathsf{poly}(S_{l-\tilde{\mathsf{id}}})$ respectively. To reach a contradiction, one must argue that the reduction B belongs to*

[18] Note that the case $\mathsf{id} = \tilde{\mathsf{id}}$ is an invalid execution and hence not considered.

$\mathcal{C}^{\vee}_{d_{\mathsf{id}},S_{l-\mathsf{id}}}$. *In other words, either* $\mathsf{dep}(A) + \mathsf{poly}(d_{\tilde{\mathsf{id}}+1})$ *is at most* $\mathsf{poly}(d_{\mathsf{id}})$ *or* $\mathsf{size}(A) + \mathsf{poly}(S_{l-\tilde{\mathsf{id}}})$ *is at most* $\mathsf{poly}(S_{l-\mathsf{id}-1})$. *Since* A *chooses both* id *and* $\tilde{\mathsf{id}}$, *this can only hold if* $\mathsf{dep}(A)$ *and* $\mathsf{size}(A)$ *are both small; that is,* $o(d_1)$ *and* $o(S_1)$ *respectively. As a result, we only show non-malleability of* $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ *against weak adversaries whose depth and size both are bounded by* $\mathsf{poly}(d_0) = o(d_1)$ *and* $\mathsf{poly}(S_0) = o(S_1)$ *respectively.*

Remark 8. *Furthermore, we note that even though* $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ *is non-malleable w.r.t. extraction, we cannot prove that it is non-malleable (w.r.t. commitment). This is because the underlying commitment schemes* $\mathsf{ECom}_{\mathsf{id}}$*'s are only over-extractable. Over-extractability guarantees that for a valid commitment, the value extracted by the extractor is indeed the value committed. However, when a commitment is invalid, the extracted value can be arbitrary – hence the name over-extractable. Therefore, there might exist an adversary* A *that depending on the value committed on the left sends invalid commitments with different probabilities on the right. Such an adversary clearly violates the non-malleability (w.r.t. commitment) but may not violate non-malleability w.r.t. extraction. This is because the over-extracted values may still be indistinguishable. Hence, we cannot base non-malleability (w.r.t. commitment) on non-malleability w.r.t. extraction of* $(\mathsf{ENMCom}, \mathsf{ENMOpen})$.

6 Strengthening Non-malleability

The scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ described in Section 5 is only stand-alone (one-one) non-malleable w.r.t. extraction. However, our final goal is to construct a scheme that is concurrent non-malleable (w.r.t. commitment). In this section, we describe a transformation that transforms any 2-round commitment scheme $\langle C, R\rangle$ which is one-one non-malleable w.r.t. extraction (against adversaries of some bounded depth and size) into a 2-round commitment scheme $\langle \widehat{C}, \widehat{R}\rangle$ which is concurrent non-malleable w.r.t. extraction as well as concurrent non-malleable (w.r.t. commitment) (against adversaries of some other bounded depth and size), while preserving the length of the identities.

We present the transformed protocol $\langle \widehat{C}, \widehat{R}\rangle$ in Section 6.3. Before that, we list the building blocks used in the transformation in Section 6.2, and we give high-level intuition on the design of the protocol $\langle \widehat{C}, \widehat{R}\rangle$ in Section 6.1. In particular, in a step by step fashion, we explain the purpose of different components in the protocol. If the reader prefers to read the actual protocol directly, please skip Section 6.1 and start from Section 6.2.

6.1 A Bare-Bone Protocol and Challenges

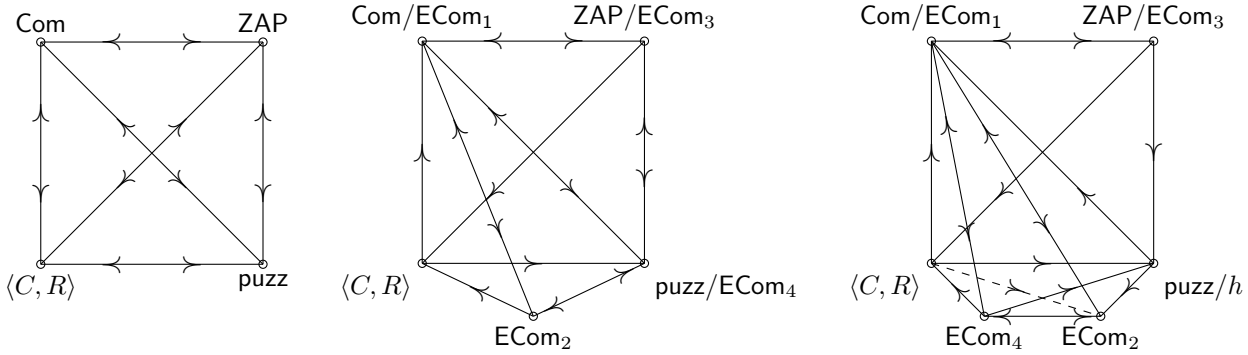
As discussed in the overview in Section 2, our construction of $\langle \widehat{C}, \widehat{R}\rangle$ is inspired by the non-malleability amplification technique in [LP09]. As a starting point, their technique suggests the following bare-bone protocol:

A Bare-Bone Protocol $\langle \widehat{C}, \widehat{R}\rangle$. The receiver sends a *puzzle* puzz. Here by puzzle we mean a computationally problem that i) is hard to solve when generated honestly, and ii) has a unique solution even when generated maliciously. For instance, a puzzle could be a random image $f(x)$ of an injective one-way function whose solution is the preimage, or a randomly sampled hash function whose solution is a collision. (In particular, this puzzle does not refer to time-lock puzzles.) In addition, the receiver also sends the first message a_{NM} of $\langle C, R\rangle$ and the first message a_{ZAP} of ZAP. The committer computes a commitment $c1$ to v using a non-interactive commitment scheme Com and sends the second message b_{NM} of $\langle C, R\rangle$ committing to a random string $r1$, and the second

message b_{ZAP} of ZAP proving that either i) $c1$ commits to v or ii) $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commits to a solution s of the puzzle puzz (which is efficiently verifiable).

$$\widehat{C} \quad \xleftarrow{\mathsf{puzz},\ a_{\mathsf{NM}},\ a_{\mathsf{ZAP}}} \quad \widehat{R}$$
$$\widehat{C} \quad \xrightarrow{\mathsf{Com}(v),\ b_{\mathsf{NM}},\ b_{\mathsf{ZAP}}} \quad \widehat{R}$$

As discussed before, to show the security of such a bare-bone protocol, *ideally*, we would like different components — puzz, $\langle C, R\rangle$, Com, and ZAP — to be *mutually non-malleable*. Informally speaking, we say that a primitive P is more secure than a primitive Q, denoted as $\mathsf{P} \succ \mathsf{Q}$, if the security of P holds even when security of Q is broken by force; P and Q are mutually non-malleable if $\mathsf{P} \prec\succ \mathsf{Q}$. The ideal configuration is illustrated in Figure 2 (i). Towards realizing as many constraints in the ideal configuration as possible, the first idea is using three size-and-depth robust commitment schemes $\mathsf{ECom}_1, \mathsf{ECom}_4, \mathsf{ECom}_3$ [19] to implement Com and puzz, and augment ZAP so that they become mutually non-malleable. But, we run into problems with respect to the input non-malleable commitment $\langle C, R\rangle$.



(i) Ideal Configuration (ii) Assume NIWI (iii) Assume CRH

Figure 2: The relation between different primitives. **(i)**: The ideal configuration where all primitives are mutually non-malleable to each other; however, it cannot be instantiated. **(ii)** A sufficient configuration; it can be instantiated assuming NIWI. **(iii)**: A sufficient configuration, which can be instantiated assuming collision resistant hash functions or one-way permutations. (The dashed line is by transitivity.)

Challenge 1: $\langle C, R\rangle$ is only secure against adversaries which have both bounded depth *AND* bounded size. (Technically, it is secure against $\mathcal{C}^{\wedge}_{d_{\mathsf{NM}}, S_{\mathsf{NM}}}$, for some d_{NM} and S_{NM}; this is the case for the basic schemes constructed in Section 5, as well as the schemes produced by the transformation in this section.) This type of *AND* security means either a primitive P is more secure than $\langle C, R\rangle$ or less, but cannot be mutually non-malleable. Though through a more careful analysis, we can remove some constraints w.r.t. the non-malleable commitment, it still requires $\langle C, R\rangle \prec\succ \mathsf{puzz}$, in order to show the security of the bare-bone protocol.

Challenge 2: In addition, constructing a puzzle from size-and-depth robust commitment ECom_4 is not straightforward. If we naively use $\mathsf{puzz} = \mathsf{ECom}_4(s)$ as a puzzle, a malicious man-in-the-middle can send an invalid commitment, which has no solution; this would make the

[19] The indexes are as such in order to match the protocol description later.

security proof stuck. To prevent this, one straightforward approach is asking the receiver to send two puzzles and prove using NIWI that at least one of them is well-formed. However, this requires relying on the existence of NIWI.

To resolve Challenge 1, we modify the bare bone protocol using an additional size-and-depth robust commitment ECom_2. The key idea is creating a "buffer" between $\langle C, R\rangle$ and puzz, by setting the following relation: $\mathsf{ECom}_2 \succ \langle C, R\rangle$, $\langle C, R\rangle \succ \mathsf{puzz}$, and $\mathsf{ECom}_2 \prec\!\!\succ \mathsf{puzz}$, as illustrated in Figure 2 (ii). Note that now the non-malleable commitment does not need to satisfy mutual non-malleability with either ECom_2 or puzz. On the other hand, the mutual non-malleability of ECom_2 and puzz helps the security proof to go through.

However, to fulfill the relation $\mathsf{ECom}_2 \prec\!\!\succ \mathsf{puzz}$, it seems necessary to instantiate puzz using a size-and-depth robust commitment scheme, which however as mentioned in Challenge 2 above would involve using NIWI to prevent a malicious receiver from sending an invalid commitment as a puzzle which has no solution. To avoid this, we would like to set puzz to be, for example, a randomly chosen collision resistant hash (CRH) function h, or a randomly chosen image $y = f(s)$ of a one-way permutation (OWP), whose corresponding solutions are respectively a collision of h and a preimage of y. These puzzles have the advantage that their validity are efficiently verifiable and hence NIWI can be disposed. But, a problem with using, say, h as the puzzle is that, it cannot be mutually non-malleable with ECom_2. To resolve this, we use a $h \succ \mathsf{ECom}_2$, and to compensate for the fact that $h \not\succ \mathsf{ECom}_2$, we use non-uniformity in the proof as follows: When reducing to the security of ECom_2, the reduction instead of finding a collision of h by force, receives a collision as a non-uniform advice. This can be done since the puzzle h is sent in the first message completely before the ECom_2 commitment.

Unfortunately, instantiating the puzzles using CRH or OWP creates another problem: Given that $\langle C, R\rangle \succ \mathsf{puzz} = h$ and $h \succ \mathsf{ECom}_2$, it actually implies that $\langle C, R\rangle \succ \mathsf{ECom}_2$. This transitivity holds because h is only secure against attackers with bounded size. (If h were replaced with another size-and-depth robust commitment ECom', then transitivity does not hold in general.) But this means $\langle C, R\rangle$ needs to be mutually non-malleable with ECom_2 again. To solve this problem, we again use the idea of creating "buffers". More specifically, we set the following relation: $\mathsf{ECom}_4 \succ \langle C, R\rangle$, $\langle C, R\rangle \succ \mathsf{puzz}$, $\mathsf{puzz} \succ \mathsf{ECom}_2$, and $\mathsf{ECom}_2 \prec\!\!\succ \mathsf{ECom}_4$, as illustrated in Figure 2 (iii). Now transitivity implies that $\langle C, R\rangle \succ \mathsf{ECom}_2$, but $\langle C, R\rangle$ no longer need to be simultanously weaker than ECom_2, and only needs to be weaker than the new "buffer" ECom_4. Moreover, the mutual non-malleability between ECom_2 and ECom_4 helps the proof to go through.

6.2 Building Blocks

Our transformation will make use of the following building blocks. We note that the parameters associated with these building blocks are set so as to satisfy the relations as depicted in Figure 2 (iii), where an arrow from primitive X to primitive Y, denoted as $X \succ Y$, means that X is harder than Y.

For some hierarchy of non-decreasing functions on $\mathbb{N}$ satisfying,

$$\begin{aligned} &n << d_4 << d_3 << d_1 << d_2 << S_2 << S_1 << S_{\mathsf{CRH}} << \\ &S'_{\mathsf{CRH}} << S_{\mathsf{NM}} << S'_{\mathsf{NM}} << S_3 << S_4 << S'_4 << S^* \ , \end{aligned} \tag{9}$$

the transformation relies on the following building blocks,

1. $\langle C, R\rangle$ is a 2-round, tag-based commitment scheme for $t(n)$-bit identities that is $(S'_{\mathsf{NM}}, S'_{\mathsf{NM}})$-over-extractable by extractor $o\mathcal{E}_{\mathsf{NM}}$. Furthermore, $\langle C, R\rangle$ is one-one $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}}, S_{\mathsf{NM}}}$-non-malleable w.r.t. extraction by $o\mathcal{E}_{\mathsf{NM}}$.[20]

2. $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_1, S_1}$-hiding and (d_2, S_{CRH})-over-extractable w.r.t. extractor $o\mathcal{E}_1$.

3. $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_2, S_2}$-hiding and (S_2, S_1)-over-extractable w.r.t. extractor $o\mathcal{E}_2$.

4. $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_3, S_3}$-hiding and (d_1, S_4)-over-extractable w.r.t. extractor $o\mathcal{E}_3$.

5. $(\mathsf{ECom}_4, \mathsf{ECom}_4)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_4, S_4}$-hiding and (d_3, S'_4)-over-extractable w.r.t. extractor $o\mathcal{E}_4$.

6. ZAP is a 2-round $\mathcal{C}^{\wedge}_{S^*, S^*}$-witness-indistinguishable proof.

7. $\mathcal{H} = \{H_n\}_{n\in\mathbb{N}}$ is a family of non-uniform $\mathcal{C}^{\wedge}_{S_{\mathsf{CRH}}, S_{\mathsf{CRH}}}$-collision resistant hash functions such that there exists a circuit in $\mathcal{C}^{\wedge}_{S'_{\mathsf{CRH}}, S'_{\mathsf{CRH}}}$ which finds collisions for $\mathcal{H}$ with probability 1.[21]

6.3 Commitment Scheme $\langle \widehat{C}, \widehat{R}\rangle$

Using building blocks described in the previous subsection, we now describe our construction of a 2-round, tag-based commitment scheme $\langle \widehat{C}, \widehat{R}\rangle$ for $t(n)$-bit identities that is (d_2, S_{CRH})-over-extractable w.r.t. an extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$, and show that it is both concurrent $\mathcal{C}^{\wedge}_{d_4, d_4}$-non-malleable w.r.t. extraction by $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ and concurrent $\mathcal{C}^{\wedge}_{d_4, d_4}$-non-malleable (w.r.t. commitment).

The committer $\widehat{C}$ and the receiver $\widehat{R}$ receive the security parameter 1^n and identity $\mathsf{id} \in \{0,1\}^{t(n)}$ as common input. Furthermore, $\widehat{C}$ gets a private input $v \in \{0,1\}^{\alpha}$ which is the value to be committed.

- Commit stage - First round:

  1. $\widehat{R}$ samples a hash function h from $\mathcal{H}_n$ uniformly at random.
  2. $\widehat{R}$ samples the first message a_{ZAP} of ZAP.
  3. $\widehat{R}$ generates the first message a_{NM} of $\langle C, R\rangle$ using the honest receiver R with identity id.
  4. $\widehat{R}$ sends $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ as the first round message to $\widehat{C}$.

- Commit stage - Second round:

  1. (a) $\widehat{C}$ computes a commitment $c1$ to the value v using ECom_1. Let $d1$ be the corresponding decommitment string.

[20] The non-interactive scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ of Section 5 can be viewed as a 2-round scheme $\langle C, R\rangle$ where the first round message from R is the null string. Also, note that $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ is stronger than what we require here – it is non-malleable against circuits in $\mathcal{C}^{\wedge}_{d,S}$ and (S', S'') over-extractable for $d << S << S' << S''$ while here $\langle \widehat{C}, \widehat{R}\rangle$ is only required to be non-malleable for circuits in $\mathcal{C}^{\wedge}_{d,d}$ and be (S,S)-over-extractable for $d << S$.

[21] We obtain the $\mathcal{C}^{\wedge}_{S_{\mathsf{CRH}}, S_{\mathsf{CRH}}}$-collision resistant family $\mathcal{H} = \{D_n\}_{n\in\mathbb{N}}$ from the $S(\lambda) = 2^{\lambda^{\varepsilon}}$-secure CRH family (for some $0 < \varepsilon < 1/2$) $\mathcal{H}' = \{H'_\lambda\}_{\lambda\in\mathbb{N}}$ (defined in Section 3.7) by setting $\lambda = (\log S_{\mathsf{CRH}}(n))^{\frac{1}{\varepsilon}}$ and letting $H_n = H'_\lambda$ where λ and n are the security parameters of $\mathcal{H}'$ and $\mathcal{H}$ respectively. See Section 8 for a rigorous discussion on instantiations of the basic building blocks required in this Section.

(b) $\widehat{C}$ computes a commitment $c3$ to the decommitment $(v, d1)$ of $c1$ using ECom_3.

2. (a) $\widehat{C}$ computes a commitment $c2$ to a random string $r1$ using ECom_2.
   (b) Given a_{NM}, $\widehat{C}$ computes the second message b_{NM} of $\langle C, R\rangle$ using the honest committer C with identity id to commit to a random string $r2$.
   (c) $\widehat{C}$ computes a commitment $c4$ to a random string $r3$ using ECom_4.
3. Given a_{ZAP}, $\widehat{C}$ computes the second message b_{ZAP} of ZAP to prove the following OR-statement:
   (a) *either* there exists a string $\bar{v}$ such that $c1$ is a commitment to $\bar{v}$ and $c3$ commits to a decommitment of $c1$.
   (b) *or* there exists a string $\bar{s} = (x_1, x_2)$ such that $c2$ is a commitment to $\bar{s}$ and $c4$ commits to a decommitment of $c2$ and $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commit to a decommitment of $c4$ and $h(x_1) = h(x_2)$.

   $\widehat{C}$ proves the statement (a) by using a decommitment of $c3$ to $(v, d1)$ — decommitment of $c1$ to v — as the witness.
4. $\widehat{C}$ sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second message to $\widehat{R}$ and keeps the decommitment $(v, d1)$ private.

- Reveal stage:
  On receiving $(v, d1)$ from $\widehat{C}$, $\widehat{R}$ accepts the decommitment if the ZAP proof is accepting and if $\mathsf{EOpen}_1(c1, v, d1) = 1$. Otherwise, it rejects.

We refer to the entire transcript of the interaction as the commitment c. Moreover, we say that an interaction (with transcript c) is *accepting* if the ZAP proof contained in the commitment c is accepting. According to the reveal stage, the value of a commitment c, $\mathsf{val}(c)$ is the value committed under $c1$ (contained in c) if c is accepting. Otherwise, $\mathsf{val}(c)$ is $\perp$.

Next, we describe the extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ of the scheme below.

- Extraction - Extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$:
  On receiving a commitment c and identity id, $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ first verifies the ZAP proof and outputs $\perp$ if the proof is not accepting. Otherwise, it runs the extractor $o\mathcal{E}_1$ on $c1$ and outputs the extracted value v'.

Theorem 12. *$\langle \widehat{C}, \widehat{R}\rangle$ is a 2-round, perfectly binding, $\mathcal{C}^{\wedge}_{d_4,d_4}$-hiding, (d_2, S_{CRH})-over-extractable commitment scheme for identities of length $t(n)$.*

Proof. The perfectly binding property follows from that of the non-interactive commitment scheme $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$. The proof of hiding will follow from the proof of Theorem 13, which we present later.

- Over-extractability: A valid commitment c to a value v, from the definition of reveal stage of $\langle \widehat{C}, \widehat{R}\rangle$, is such that the ZAP proof contained in c is accepting and $c1$ (contained in c) is a valid commitment to v using ECom_1. In this case, the extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ runs $o\mathcal{E}_1$ on $c1$, which by the over-extractability of ECom_1 w.r.t. $o\mathcal{E}_1$, outputs v with . Thus, $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ extracts outputs $\mathsf{val}(c)$ for any valid commitment c. Moreover, $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ belongs to the class $\mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, since $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ and the rest of computation by $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ takes $\mathsf{poly}(n)$ time. Hence, the scheme $\langle \widehat{C}, \widehat{R}\rangle$ is (d_2, S_{CRH})-over-extractable.

□

Next, we establish the non-malleability of the scheme $\langle \widehat{C}, \widehat{R} \rangle$.

Theorem 13. *$\langle \widehat{C}, \widehat{R} \rangle$ is concurrent $\mathcal{C}^{\wedge}_{d_4,d_4}$-non-malleable w.r.t. extraction by extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$.*

Theorem 14. *$\langle \widehat{C}, \widehat{R} \rangle$ is concurrent $\mathcal{C}^{\wedge}_{d_4,d_4}$-non-malleable (w.r.t. commitment).*

In order to prove concurrent non-malleability w.r.t. commitment, Lin, Pass and Venkitasubramaniam [LPV08] showed that it is sufficient to prove non-malleability against adversaries participating in one left interaction and many right interactions. We refer to such an adversary as a *one-many* adversary. More precisely, they presented a reduction that, given an adversary A and a distinguisher D that break concurrent non-malleability, builds a one-many adversary $\widetilde{A}$ and a distinguisher $\widetilde{D}$ that violate one-many non-malleability. Their reduction blows up the size and the depth of the adversary $\widetilde{A}$ and the distinguisher $\widetilde{D}$ (over A and D respectively) by a $\mathsf{poly}(n)$ factor and thereby incurs a polynomial loss in security. We claim that the same reduction applies to the new notion of non-malleability w.r.t. extraction, therefore establishing that one-many non-malleability w.r.t. extraction implies concurrent non-malleability w.r.t. extraction. Moreover, we consider non-malleability (w.r.t. commitment and extraction) against circuit classes $\mathcal{C}$ which are closed under composition with $\mathcal{P}/\mathrm{poly}$, hence their reduction preserves security in terms of the circuit class against which (concurrent and one-many) non-malleability is considered — a $\mathcal{C}$-one-many non-malleable commitment scheme is $\mathcal{C}$-concurrent non-malleable. We state the extended version of their theorem below. The proof follows syntactically from the proof of Proposition 1 in [LPV08] but for completeness we also include the formal proof in Appendix 11.1.

Theorem 15 (one-many to concurrent [LPV08])**.** *Let $\langle \widehat{C}, \widehat{R} \rangle$ be a commitment scheme and $\mathcal{C}$ be a class of circuits that is closed under composition with $\mathcal{P}/\mathrm{poly}$.*

1. *If $\langle \widehat{C}, \widehat{R} \rangle$ is one-many $\mathcal{C}$-non-malleable then it is concurrent $\mathcal{C}$-non-malleable.*
2. *If $\langle \widehat{C}, \widehat{R} \rangle$ is one-many $\mathcal{C}$-non-malleable w.r.t. extraction (by extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$) then it is concurrent $\mathcal{C}$-non-malleable w.r.t. extraction (by $\widehat{o\mathcal{E}}_{\mathsf{NM}}$).*

Proof of Theorem 13,14. We now proceed to prove Theorem 13, 14. Let us consider a fixed family of circuits $A = \{A_n\}_{n\in\mathbb{N}}$ belonging to the class $\mathcal{C}^{\wedge}_{d_4,d_4}$ which participates in one left interaction and $m = \mathsf{poly}(n)$ right interactions while sending/receiving commitments to values of length $\alpha = \mathsf{poly}(n)$-bits. By Theorem 15, to show Theorems 13, 14, it suffices to prove the the following:

$$\left\{\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 0)\right\}_n \approx_c \left\{\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 1)\right\}_n \tag{10}$$

$$\left\{\mathsf{mim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 0)\right\}_n \approx_c \left\{\mathsf{mim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 1)\right\}_n \tag{11}$$

We prove the above indistinguishability via a sequence of hybrids $\{H_j(b)\}_{0\le j\le 6}$ for $b \in \{0,1\}$, where $H_0(b)$ is identical to an honest man-in-the-middle execution $\mathsf{MIM}(1^n, b)$ with A, and $H_j(b)$ for each $1 \le j \le 6$ runs a man-in-the-middle execution with A where the left interaction is gradually simulated. For notational convenience, we use the convention x to denote a random variable in the left interaction, and convention $\tilde{x}_i$ to denote the corresponding random variable in the i'th right interaction. For example, h denotes the hash function sent by A in the left interaction, while $\tilde{h}_i$ denotes that sent by the honest receiver in the i'th right interaction. Moreover, for each hybrid

$H_j(b)$, we denote by $\mathsf{mim}^A_{H_j}(b)$ (and respectively, $\mathsf{emim}^A_{H_j}(b)$) the random variables that describe the view of A and the values $\{\widetilde{v}_i\}_{i\in[m]}$ committed to in (or respectively, $\{\widetilde{v}'_i\}_{i\in[m]}$ extracted from) the right interactions. Again, for every right interaction i, if the interaction is not accepting or its identity $\widetilde{\mathsf{id}}_i$ equals to the left identity id, then $\widetilde{v}'_i = \widetilde{v}_i = \perp$; we say that a right interaction is *successful* if this case does not happen.

To show indistinguishability as described in Equation (11) and (10), we prove in Lemma 2 that the view of A and the values extracted from right interactions are indistinguishable in neighboring hybrids $H_j(b)$ and $H_{j+1}(b)$ for the same b, and statistically close in $H_6(1)$ and $H_5(0)$ — this establishes Equation (10). Furthermore, we show that in every hybrid $H_j(b)$, values extracted from right interactions are actually identical to the actual values committed in right interactions, except with negligible probability. This shows that the emim and mim random variables are statistically close (as stated in Lemma 3) and hence establishes Equation (11).

Lemma 2. *For $b \in \{0,1\}$ and $0 \le j \le 5$, the following are computationally indistinguishable,*

$$\mathsf{emim}^A_{H_j}(b) \;;\; \mathsf{emim}^A_{H_{j+1}}(b)\ ,$$

and $\mathsf{emim}^A_{H_0}(b) = \mathsf{emim}^A_{\langle \widehat{C},\widehat{R}\rangle}(b)$ and $\mathsf{emim}^A_{H_6}(b) \approx_s \mathsf{emim}^A_{H_5}(0)$.

Lemma 3. *For $b \in \{0,1\}$ and $0 \le j \le 6$, the following are statistically close,*

$$\mathsf{emim}^A_{H_j}(b) \;;\; \mathsf{mim}^A_{H_j}(b).$$

Towards proving the above two lemmas, we will maintain a *soundness invariant* throughout all hybrids. Recall that the protocol requires a committer to prove using ZAP that one of the following two statements is true; we refer to the first as the honest statement and the second as the fake statement.

The honest statement: either it has committed to v in $c1$ (of ECom_1) and to a decommitment $(v, d1)$ of $c1$ in $c3$ (of ECom_3),

The fake statement: or it has committed to a collision $s = (x_1, x_2)$ of the hash function h in $c2$ (of ECom_2), to a decommitment $(s, d2)$ of $c2$ in $c4$ (of ECom_4), and to a decommitment $((s, d2), d4)$ of $c4$ in $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ (of $\langle C, R\rangle$).

No-fake-witness Invariant. We say that A commits to a fake witness in a right interaction i, if the value committed by A in the non-malleable commitment $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ (i.e., $\mathsf{val}((\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i}))$) is a decommitment $((\tilde{s}_i, \tilde{d2}_i), \tilde{d4}_i)$ of $\tilde{c4}_i$ such that $\tilde{s}_i$ is a collision of $\tilde{h}_i$ and $(\tilde{s}_i, \tilde{d2}_i)$ is a decommitment of $\tilde{c2}_i$.

Invariant 1 (No-fake-witness invariant)**.** *In $H_j(b)$, the probability that there exists a right interaction i that is successful and A commits to a fake witness in it is negligible.*

We show below that this invariant holds in all hybrids. The reason that we maintain Invariant 1 is that it enforces the man-in-the-middle attacker to always prove the honest statement in every successful right interaction. When this is the case, we show that the values extracted from the right interactions are identical to the values committed to in the right interactions except from negligible probability. Formally,

Claim 1. *In every hybrid $H_j(b)$, if Invariant 1 holds, then* $\mathsf{emim}^A_{H_j}(b)$ *and* $\mathsf{mim}^A_{H_j}(b)$ *are statistically close.*

At a high level, Claim 1 follows from the soundness of ZAP and over-extractability of the commitment scheme $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$. Since, Invariant 1, holds, A does not commit to a fake witness in any successful right interaction. This by the soundness of ZAP implies that A proves the honest statement which inturn, implies that commitment $\tilde{c1}_i$ is valid. By over-extractability of ECom_1 it follows that the value extracted from $\tilde{c1}_i$ (corresponds to emim) is indeed identical to the $\mathsf{val}(\tilde{c1}_i)$ which, by definition, is the value of the i-th right commitment (corresponds to mim). We detail a more formal proof in Section 6.4.

Moving ahead, by Claim 1 it is clear that showing Lemma 3 boils down to establishing Invariant 1. Towards this goal we further observe that Invariant 1 follows from the following invariant which will be easier to prove. Instead of reasoning about A committing to a fake witness, we keep the invariant that the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is NOT a fake witness.

Invariant 2. *In $H_j(b)$, the probability that there exists a right interaction i that is successful and the value* extracted *from the non-malleable commitment $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ in this interaction is a fake witness is negligible.*

Claim 2. *In every hybrid $H_j(b)$, if Invariant 2 holds, then Invariant 1 also holds except with negligible probability.*

Proof. For every right interaction k, consider two cases:

- If the non-malleable commitment $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$ in this right interaction is valid, by the over-extractability property of $\langle C, R\rangle$ w.r.t. extractor $o\mathcal{E}_{\mathsf{NM}}$ the value extracted from it is exactly equal to the value committed, . Therefore, if the value *extracted* is not a fake witness, neither is the value *committed*.
- If the non-malleable commitment $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$ is not valid, the value committed is $\perp$ and cannot be a fake witness.

Hence, Invariant 2 implies Invariant 1. □

Combining the above two claims, we have,

Lemma 4. *For $b \in \{0,1\}$ and $0 \le j \le 6$, if Invariant 2 holds in hybrid $H_j(b)$ then* $\mathsf{emim}^A_{H_j}(b)$ *and* $\mathsf{mim}^A_{H_j}(b)$ *are statistically close.*

Therefore, to show Theorem 13 and Theorem 14, it boils down to prove Lemma 2 and that Invariant 2 holds in all hybrids. Next, we describe our hybrids $\{H_j(b)\}_{0\le j\le 6}$ and show that Lemma 2 and Invariant 2 indeed hold. In this Section, we only give high level proofs of the Claims and direct the reader to Section 6.4 for formal proofs.

Hybrid $H_0(b)$: Hybrid $H_0(b)$ emulates an honest MIM execution $\mathsf{MIM}^A_{\langle \widehat{C}, \widehat{R}\rangle}(b)$ with A on the challenge bit b by honestly committing to the value v_b on the left and simulating honest receivers on the right.[22] Therefore,

$$\mathsf{emim}^A_{H_0}(b) = \mathsf{emim}^A_{\langle \widehat{C}, \widehat{R}\rangle}(b) \ .$$

[22] Recall that A in the MIM execution $\mathsf{MIM}^A_{\langle \widehat{C}, \widehat{R}\rangle}(b)$ sends (v_0, v_1) on the left and receives a commitment to v_b.

Next, we show that Invariant 2 holds in $H_0(b)$. In fact we show that the value extracted from the ECom_2 commitment $\widetilde{c2}_k$ in any right interaction k is not a collision of the hash function $\widetilde{h}_k$, which implies Invariant 2. At a high level this readily follows from the fact that the collision-resistance of the hash function is more secure than ECom_2, $h \succ \mathsf{ECom}_2$ (see Figure 2 (iii)). This is because if in some right interaction k, the attack commits to a collision of $\widetilde{h}_k$ using ECom_2, then we can construct a non-uniform circuit that violates the collision-resistance of $\widetilde{h}_k$ by extracting from $\widetilde{c2}_k$. A formal proof can be found in Section 6.4.

Claim 3. *For $b \in \{0,1\}$ and for every right interaction i in $H_0(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Hybrid $H_1(b)$: Hybrid $H_1(b)$ proceeds identically to $H_0(b)$ except that the ECom_2 commitment $c2$ sent to A in the left interaction is generated differently. In $H_0(b)$, $c2$ is a commitment to a random string $r1$ whereas in $H_1(b)$ $c2$ is a commitment to the lexicographically first collision s of the hash function h (received as non-uniform advice). The rest of the execution is simulated identically to $H_0(b)$.

First, we show that Invariant 2 holds in $H_1(b)$. In fact we show that the value extracted from the ECom_4 commitment $\widetilde{c4}_k$ in any right interaction k is not a decommitment of $\widetilde{c2}_k$ to a collision of the hash function $\widetilde{h}_k$, which implies Invariant 2. At a high level this follows from the fact that ECom_2 is more secure than ECom_4, $\mathsf{ECom}_2 \succ \mathsf{ECom}_4$ (see Figure 2 (iii)), and the trick that the reduction can receive a collision of h as a non-uniform advice. Suppose that in $H_1(b)$, the value extracted from $\widetilde{c4}_k$ in some right interaction k satisfies the condition above with $1/\mathsf{poly}(n)$ probability. By Claim 3, this happens with only negligible probability in $H_0(b)$. Then we can construct a non-uniform circuit that violates the hiding of ECom_2 by extracting from $\widetilde{c4}_k$. We give a formal proof in Section 6.4.

Claim 4. *For $b \in \{0,1\}$ and for every right interaction i in $H_1(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_0}(b)$ and $\mathsf{emim}^A_{H_1}(b)$ are indistinguishable, that is, view of A and the values extracted from ECom_1 commitments in every successful right interaction are indistinguishable in $H_0(b)$ and $H_1(b)$. This essentially follows from the same proof as Claim 4, but now relying on the fact that ECom_2 is more secure than ECom_1, $\mathsf{ECom}_2 \succ \mathsf{ECom}_1$ (see Figure 2 (iii)). We give a formal proof in Section 6.4.

Claim 5. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_0}(b); \mathsf{emim}^A_{H_1}(b) \ .$$

Hybrid $H_2(b)$: Hybrid $H_2(b)$ proceeds identically to $H_1(b)$ except that the ECom_4 commitment $c4$ sent to A in the left interaction is generated differently. In $H_1(b)$, $c4$ is a commitment to a random string $r3$ whereas in $H_2(b)$ $c4$ is a commitment to a decommitment of $c2$ to a collision s of the hash function h. More precisely, $H_2(b)$ first finds a collision s for the function h and then commits to s using ECom_2 under $c2$. Then it commits to the decommitment of $c2$ under $c4$. The rest of the execution is simulated identically to $H_1(b)$.

First, we show that Invariant 2 holds in $H_2(b)$. At a high level this follows from the fact that ECom_4 is more secure than $\langle C, R\rangle$, $\mathsf{ECom}_4 \succ \langle C, R\rangle$ (see Figure 2 (iii)). Suppose that

Invariant 2 does not hold in $H_2(b)$. This means that the value extracted from the non-malleable commitment in some right interaction k is a fake witness with probability $1/\mathsf{poly}(n)$ in $H_2(b)$, but negligible in $H_1(b)$ by Claim 4. Then, we can construct a non-uniform circuit B that violates the hiding of ECom_4 by extracting from the non-malleable commitment. One slight difference from the proof of Claim 4 is that since ECom_4 is also more secure than h, $\mathsf{ECom}_4 \succ h$ (see Figure 2 (iii)), the reduction B can afford to find collision of h internally, instead of receiving it as a non-uniform advice. We give a formal proof in Section 6.4.

Claim 6. *For $b \in \{0,1\}$ and for every right interaction i in $H_2(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_1}(b)$ and $\mathsf{emim}^A_{H_2}(b)$ are indistinguishable, that is, view of A and the values extracted from ECom_1 commitments in every successful right interactions are indistinguishable in $H_1(b)$ and $H_2(b)$. The proof is essentially the same as that for Claim 6, except it now relies on the fact that $\mathsf{ECom}_4 \succ \mathsf{ECom}_1$ (and $\mathsf{ECom}_4 \succ h$; see Figure 2 (iii)). We give a formal proof in Section 6.4.

Claim 7. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_1}(b); \mathsf{emim}^A_{H_2}(b) \ .$$

Hybrid $H_3(b)$: Hybrid $H_3(b)$ proceeds identically to $H_2(b)$ except that the second message b_{NM} of $\langle C, R\rangle$ sent to A in the left interaction is generated differently. In $H_2(b)$, b_{NM} is such that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commits to a random string $r2$ whereas in $H_3(b)$ b_{NM} is such that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commits to a decommitment of $c4$ to a decommitment of $c2$ to a collision s of the hash function h. More precisely, $H_3(b)$ generates a commitment $c2$ to the collision s (obtained by brute-force search). Let $d2$ be the corresponding decommitment string. Then, $H_3(b)$ computes the commitment $c4$ to the decommitment $(s, d2)$ of $c2$. Let $d4$ be the corresponding decommitment string. Then, given a_{NM}, $H_3(b)$ computes the second message b_{NM} to commit to $((s, d2), d4)$. The rest of the execution is simulated identically to $H_2(b)$.

First, we show that Invariant 2 holds in $H_3(b)$. At a high-level, this follows from the one-one non-malleability w.r.t. extraction of $\langle C, R\rangle$. Suppose that Invariant 2 does not hold in $H_3(b)$ then there exists a right interaction k such that the probability that it is successful and the value extracted the non-malleable commitment contained in this interaction is a fake witness is $1/\mathsf{poly}(n)$ in $H_3(b)$ and is negligible in $H_2(b)$ (by Claim 6). This violates the one-one non-malleability w.r.t. extraction of $\langle C, R\rangle$ as we formally show below. We give a formal proof in Section 6.4.

Claim 8. *For $b \in \{0,1\}$ and for every right interaction i in $H_3(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_2}(b)$ and $\mathsf{emim}^A_{H_3}(b)$ are indistinguishable, that is, view of A and the values extracted from ECom_1 commitments in every successful right interactions are indistinguishable in $H_2(b)$ and $H_3(b)$. This follows from the fact that $\langle C, R\rangle$ is more secure than ECom_1, $\langle C, R\rangle \succ \mathsf{ECom}_1$ (see Figure 2 (iii)). Therefore, if the distribution of values extracted from the ECom_1 commitments in the right interactions are distinguishable in $H_2(b)$ and $H_3(b)$, one can construct reduction that violates the hiding of $\langle C, R\rangle$ by extracting from the ECom_1 commitments on the right. We give a formal proof in Section 6.4.

Claim 9. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_2}(b); \mathsf{emim}^A_{H_3}(b) \ .$$

Hybrid $H_4(b)$: Hybrid $H_4(b)$ proceeds identically to $H_3(b)$ except that the second message b_{ZAP} of ZAP sent to A in the left interaction is generated differently. In $H_3(b)$, b_{ZAP} is computed by proving that $c3$ commits to a decommitment $(v_b, d1)$ of $c1$ whereas in $H_4(b)$ b_{ZAP} is computed by proving that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commits to $((s, d2), d4)$ which is a decommitment of $c4$ to a decommitment $(s, d2)$ of $c2$ to the collision s of the hash function h.

First, we show that Invariant 2 holds in $H_4(b)$. At a high-level, this follows from the witness indistinguishability of ZAP, which holds against subexp-sized attackers. Since $\langle C, R\rangle$ can be broken in the time that ZAP is secure against, changing the ZAP proof on the left should not change the distribution of values extracted from the right non-malleable commitments. As the values extracted from right non-malleable commitments are not fake witnesses in $H_3(b)$ (by Claim 8), the same holds for these values in $H_4(b)$. We give a formal proof in Section 6.4.

Claim 10. *For $b \in \{0,1\}$ and for every right interaction i in $H_4(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_3}(b)$ and $\mathsf{emim}^A_{H_4}(b)$ are indistinguishable, that is, view of A and the values extracted from ECom_1 commitments in every successful right interactions are indistinguishable in $H_3(b)$ and $H_4(b)$. This follows from essentially the same proof of Claim 10, except that now we use the fact that ZAP is more secure than ECom_1. We give a formal proof in Section 6.4.

Claim 11. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_3}(b); \mathsf{emim}^A_{H_4}(b) \ .$$

Hybrid $H_5(b)$: Hybrid $H_5(b)$ proceeds identically to $H_4(b)$ except that the ECom_3 commitment $c3$ sent to A in the left interaction is generated differently. In $H_4(b)$ $c3$ is committing to the decommitment $(v_b, d1)$ of $c1$ whereas in $H_5(b)$ $c3$ is committing to 0^l where l is the length of the decommitment of $c1$. More precisely, $H_5(b)$ computes $(c1, c2, c4, b_{\mathsf{NM}})$ identically to $H_4(b)$. Then, $H_5(b)$ computes the ECom_3 commitment $c3$ to commit to 0^l. The rest of the execution is simulated identically to $H_4(b)$.

First, we show that Invariant 2 holds in $H_5(b)$. This follows from the fact that $\mathsf{ECom}_3 \succ \langle C, R\rangle$, (see Figure 2 (iii)). Suppose that Invariant 2 does not hold in $H_5(b)$ but holds in $H_4(b)$ by Claim 10, then there exists a right interaction k such that the probability that it is successful and the value extracted from the non-malleable commitment in it is a fake witness jumps from negligible in $H_4(b)$ to $1/\mathsf{poly}(n)$ in $H_5(b)$. Then, we can construct a reduction that violates the hiding of ECom_3 by extracting from the non-malleable commitment in the kth right interaction. We give a formal proof in Section 6.4.

Claim 12. *For $b \in \{0,1\}$ and for every right interaction i in $H_5(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_4}(b)$ and $\mathsf{emim}^A_{H_5}(b)$ are indistinguishable, that is, view of A and the values extracted from ECom_1 commitments in every successful right interactions are indistinguishable in $H_4(b)$ and $H_5(b)$. This follows from the same proof as that of Claim 12, except that now it relies on the fact that $\mathsf{ECom}_3 \succ \mathsf{ECom}_1$. We give a formal proof in Section 6.4.

Claim 13. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_4}(b); \mathsf{emim}^A_{H_5}(b) \ .$$

Hybrid $H_6(b)$: Hybrid $H_6(b)$ proceeds identically to $H_5(b)$ except that the ECom_1 commitment $c1$ sent to A in the left interaction is generated differently. In $H_5(b)$, $c1$ is committing to the value v_b whereas in $H_6(b)$ $c1$ is committing to the value v_0 instead where (v_0, v_1) are the values sent by A in the left interaction. The rest of the execution is simulated identically to $H_5(v)$.

First, note that for $b \in \{0,1\}$ $H_6(b)$ is in fact identical to $H_5(0)$. Therefore by Claim 12 that Invariant 2 holds in $H_5(0)$, we directly have that it holds also in $H_6(b)$.

Claim 14. *For $b \in \{0,1\}$ and for every right interaction i in $H_6(b)$, the probability that i is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we show that $\mathsf{emim}^A_{H_5}(b)$ and $\mathsf{emim}^A_{H_6}(b)$ are indistinguishable. This follows from the fact that ECom_1 is more secure than ECom_3, $\mathsf{ECom}_1 \succ \mathsf{ECom}_3$ (see Figure 2 (iii)), and the fact that Invariant 2 holds in both $H_5(b)$ and $H_6(b)$. The latter ensures that in every successful right interaction k, the attacker must prove the honest statement using ZAP that $c\tilde{3}_k$ is valid committing to a valid decommitment of $c\tilde{1}_k$ in that right interaction. Therefore, in every successful right interaction k, the value extracted from $c\tilde{3}_k$ and $\widetilde{c1}_k$ are identical. This implies that if the emim random variables are distinguishable in $H_5(b)$ and $H_6(b)$, the values extracted from the right ECom_3 commitments are also distinguishable. Then, we can construct a reduction that violates the hiding of ECom_1 by extracting from the right ECom_3 commitments. We give a formal proof in Section 6.4.

Claim 15. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{emim}^A_{H_5}(b); \mathsf{emim}^A_{H_6}(b) \ .$$

This concludes the proof of Theorem 13 and Theorem 14. We direct the reader to Section 6.4 for the formal proofs of Claims in this Section.

6.4 Proofs of Claims from Section 6.3

In this Section, we provide formal proofs of Claims from Section 6.3.

Proof of Claim 1 To show that $\mathsf{emim}^{A}_{H_j}(b)$ and $\mathsf{mim}^{A}_{H_j}(b)$ are statistically close, it suffices to argue that in $H_j(b)$, in every right interaction i, the values $\widetilde{v}'_i$ extracted from this right interaction is identical to the value $\widetilde{v}_i$ committed in this right interaction, except with negligible probability. Then the claim follows by taking a union bound over all $m = \mathsf{poly}(n)$ right interactions.

Firstly, note that if a right interaction i is not successful, then clearly $\widetilde{v}'_i = \widetilde{v}_i = \bot$. For a successful right interaction i, by the definition of extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$, $\widetilde{v}'_i$ is the value extracted by $o\mathcal{E}_1$ from the ECom_1 commitment $\widetilde{c1}_i$. Next, since Invariant 1 holds, we claim (proof presented shortly) that A proves the honest statement in successful right interactions except with negligible probability. That is,

Claim 16. *In $H_j(b)$ if Invariant 1 holds then the probability that there exists a right interaction i that is successful and A proves the fake statement in it is negligible.*

Since the honest statement is true in this right interaction i except with negligible probability, this implies that the ECom_1 commitment $\widetilde{c1}_i$ is valid. By the over-extractability of ECom_1 w.r.t. extractor $o\mathcal{E}_1$, the value extracted from $\widetilde{c1}_i$ (i.e., $\tilde{v}'_i$ in this case) is identical to the committed value $\tilde{v}_i$. Or equivalently, $\tilde{v}'_i = \tilde{v}_i$. Therefore, under Invariant 1, the random variable $\mathsf{emim}^{A}_{H_j}(b)$ is identical to $\mathsf{mim}^{A}_{H_j}(b)$, except with negligible probability. To conclude the proof of Claim 1, we now discuss the proof of Claim 16 below.

Proof of Claim 16 Let us assume that for $H_j(b)$ there exists a polynomial $p(\cdot)$ such that for infinitely many $n \in \mathbb{N}$ there exists some right interaction k that is successful and A proves the fake statement in this interaction with probability $1/p(n)$. Since Invariant 1 holds, A does not commit to the fake witness in this right interaction, except with negligible probability, which implies that the fake statement is false. Therefore, it must be that with probability at least $1/2p(n)$, the fake statement is false yet A proves the fake statement in this successful right interaction k. Given this we construct a cheating prover $\mathcal{P}^* = \{\mathcal{P}^*_n\}_{n\in\mathbb{N}}$ that breaks the soundness of ZAP with probability at least $1/2p(n)$.

$\mathcal{P}^*_n$ has k hardwired in it, participates in an interaction with the honest verifier of $\mathcal{V}$ of ZAP, internally runs A and simulates the left interaction with A as a honest committer and all right interactions except the k-th interaction as a honest receiver. For the k-th interaction, $\mathcal{P}^*$ samples a random $\widetilde{h}_k$ and the first message $\widetilde{a}_{\mathsf{NM}k}$. It sets $\widetilde{a}_{\mathsf{ZAP}k} = \mathsf{a}$ where a is the first message received by $\mathcal{P}^*$ from the honest verifier. It sends $(\widetilde{h}_k, \widetilde{a}_{\mathsf{NM}k}, \widetilde{a}_{\mathsf{ZAP}k})$ as the first message to A for its k-th right interaction. On receiving the second message from A in the k-th right interaction, $\mathcal{P}^*$ forwards the second message $\widetilde{b}_{\mathsf{ZAP}k}$ of ZAP in the k-th right interaction as its second message $\mathsf{b} = \widetilde{b}_{\mathsf{ZAP}k}$ to the honest verifer. Then, with probability at least $1/2p(n)$ the ZAP proof (a, b) is accepting and A proves the fake statement while not committing to the fake witness. This contradicts the adaptive soundness of ZAP. □

Proof of Claim 3 We show that in $H_0(b)$ the probability that there exists a right interaction k that is successful and the value extracted from $\widetilde{c2}_k$ is a collision of the hash function $\widetilde{h}_k$ in this right interaction — refer to this event as bad — is negligible. Then the claim follows, since whenever the value extracted from the non-malleable commitment in a successful right interaction k is indeed a fake witness (refer to this event as bad_1) then the commitment $\widetilde{c2}_k$ is valid and furthermore $\widetilde{c2}_k$ commits to a collision $\widetilde{s}_k$ of the hash function $\widetilde{h}_k$. By the over-extractability of ECom_2 the value extracted from $\widetilde{c2}_k$ is indeed $\widetilde{s}_k$. In other words, the claim follows because conditioned on event bad_1 occuring, the event bad occurs.

Now suppose for contradiction that there exists $b \in \{0, 1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ event bad occurs with probability $1/p(n)$ in $H_0(b)$. Or equivalently, for all

such n's there exists some right interaction k for which k is successful and the value extracted from $\widetilde{c2}_k$ is a collision of hash function $\widetilde{h}_k$ with probability at least $1/p(n)$.

Then, using A, we construct a non-uniform circuit $B = \{B_n\}_{n\in\mathbb{N}} \in \mathcal{C}_{S_{\mathsf{CRH}}}$ that outputs a collision for a hash function sampled from honestly from $\mathcal{H}$ (using D_n) with probability at least $1/p(n)$. More concretely, B with k hard-wired in it, on receiving an honestly sampled hash function h^*, emulates $H_0(b)$ for A except for the kth right interaction. In the kth right interaction, B honestly computes the first message $\widetilde{a}_{\mathsf{NM}k}$ of $\langle C, R\rangle$ and the first message $\widetilde{a}_{\mathsf{ZAP}k}$ of ZAP (as in $H_0(b)$) and sends the tuple $(\widetilde{h}_k = h^*, \widetilde{a}_{\mathsf{ZAP}k}, \widetilde{a}_{\mathsf{NM}k})$ as its first round message to A. On receiving the second round message from A in the kth interaction, B runs the extractor $o\mathcal{E}_2$ on $\widetilde{c2}_k$ and returns the extracted value as its output (irrespective of whether the right interaction k is successful or not). Note that B perfectly emulates $H_0(b)$ for A as the distribution of hash function received by B is identical to the distribution of the hash function sent by the honest receiver $\widehat{R}$ of $\langle \widehat{C}, \widehat{R}\rangle$. Then by our hypothesis, the extracted value is a collision of the function $\widetilde{h}_k = h^*$ with probability at least $1/p(n)$.

Furthermore, we argue that B belongs to the circuit class $\mathcal{C}_{S_{\mathsf{CRH}}}$: B internally runs A and $o\mathcal{E}_2$, and the rest of computation performed by B for emulating $H_0(b)$ takes $\mathsf{poly}(n)$ time. Since $o\mathcal{E}_2 \in \mathcal{C}^{\wedge}_{S_2,S_1}$ and $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ we have,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{size}(o\mathcal{E}_2) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(S_1)\\ &< \mathsf{poly}(S_{\mathsf{CRH}}) \qquad (\text{since, } S_{\mathsf{CRH}} >> d_4, S_1 \text{ from Equation (9)})\end{aligned}$$

Thus, B belongs to the class $\mathcal{C}^{\wedge}_{S_{\mathsf{CRH}},S_{\mathsf{CRH}}}$ which contradicts collision-resistance of $\mathcal{H}$. □

Proof of Claim 4 We show that in $H_1(b)$ the probability that there exists a right interaction k that is successful and the value extracted from $\tilde{c4}_k$ is a decommitment of $\tilde{c2}_k$ to a collision of the hash function $\tilde{h}_k$ in this right interaction — refer to this event as bad — is negligible. Then the claim follows, since whenever the value extracted from the non-malleable commitment in a successful right interaction k is indeed a fake witness (refer to this event as bad_1) then the commitment $\widetilde{c4}_k$ is valid and furthermore $\widetilde{c4}_k$ commits to a decommitment of $\tilde{c2}_i$ to a collision $\widetilde{s}_k$ of the hash function $\widetilde{h}_k$. Then, by the over-extractability of ECom_4 we know that the value extracted from $\widetilde{c4}_k$ is indeed a decommitment of $\tilde{c2}_k$ to a collision $\widetilde{s}_k$ of hash function $\widetilde{h}_k$. In other words, the claim follows because conditioned on event bad_1 occuring, the event bad occurs.

Towards bounding the probability of bad, first observe that by if bad occurs then for some right interaction k, $\tilde{c2}_k$ must be a valid commitment and therefore extractor $o\mathcal{E}_2$ finds a collision $\tilde{s}_k$. Then, by Claim 3 we can conclude that the bad occurs in $H_0(b)$ only with negligible probability.

Now suppose for contradiction that there exists $b \in \{0,1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ the event bad occurs with probability $1/p(n)$ in $H_1(b)$. Or equivalently, for all such n's there exists some right interaction k such that k is successful and the value extracted from $\widetilde{c4}_k$ is a decommitment of $\widetilde{c2}_k$ to a collision of hash function $\widetilde{h}_k$ with probability at least $1/p(n)$. Consider the set Γ of prefixes of transcripts up to the point where the first message in the left interaction is sent. By a standard averaging argument, there must exist a $1/2p(n)$ fraction of prefixes ρ in Γ, such that, conditioned on ρ occurring in $H_1(b)$, the probability that bad occurs is at least $1/2p(n)$. Therefore, there exist at least a $1/3p(n)$ fraction of prefixes ρ in Γ, such that, conditioned on ρ occurring in both $H_0(b)$ and $H_1(b)$, the probability that bad occurs increases by at least $1/3p(n)$ across hybrids. Fix one such prefix ρ; let h be the hash function contained in the first message in the left interaction in ρ and $s = (x_1, x_2)$ be the lexicographically first collision of h.

Then, using A, the prefix ρ and its collision s, we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_2,S_2}$ that violates the hiding of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$ with advantage at least $1/3p(n)$.

The circuit B with k, ρ, and s hard-wired in it, participates in the hiding game of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$ and internally emulates an execution of $H_1(b)$ with A as follows: [23]

- Step 1: Feed A with messages in ρ; let $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ be the left first message.
- Step 2: It samples a random string $r1$, sends $r1$ and $s = (x_1, x_2)$ as challenges in the hiding game of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$, and receives a commitment c^* to either $r1$ or s.
- Step 3: B generates the second message of the left interaction identically to $H_1(b)$ except that it embeds c^* as the ECom_2 commitment in the message. That is, B computes $(c1, c3, c4, b_{\mathsf{NM}})$ as in $H_1(b)$ (and $H_0(b)$) and then computes the second message of ZAP (b_{ZAP}) by setting $c2 = c^*$ using the honest witness as done in $H_1(b)$. It then sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message in the left interaction to A.
- Step 4: Once, B receives the second round message in the kth right interaction, if the interaction is not successful then B outputs 0. Otherwise, it runs the extractor $o\mathcal{E}_4$ on $\tilde{c4}_k$ and outputs 1 iff the extracted value is a decommitment of $\tilde{c2}_k$ to a collision of the function $\tilde{h}_k$ in right interaction k.

It is easy to see that if B receives a commitment to the random string $r1$, then it is perfectly emulates $H_0(b)$ conditioned on ρ occurring for A and if it receives a commitment to the solution s which is a collision of h then it perfectly emulates $H_1(b)$ conditioned on ρ occurring for A. As argued before, the probability that bad occurs increases by at least $1/3p(n)$. Therefore, B has advantage at least $1/3p(n)$ in violating the hiding of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$.

Moreover, we show that $B \in \mathcal{C}^{\vee}_{d_2,S_2}$: B internally runs $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, $o\mathcal{E}_4 \in \mathcal{C}^{\wedge}_{d_3,S'_4}$, and the rest of the computation done by B takes $\mathsf{poly}(n)$ time. Thus,

$$\begin{aligned}
\mathsf{dep}(B) &\leq \mathsf{dep}(A) + \mathsf{dep}(o\mathcal{E}_4) + \mathsf{poly}(n) \\
&\leq \mathsf{poly}(d_4) + \mathsf{poly}(d_3) \\
&< \mathsf{poly}(d_2) \qquad (\text{since, } d_2 >> d_4, d_3 \text{ from Equation (9)})
\end{aligned}$$

and $\mathsf{size}(B) = \mathsf{poly}(S'_4) < \mathsf{poly}(S^*)$. Therefore, B belongs to the circuit class $\mathcal{C}_{d_2}$ (resp., $B \in \mathcal{C}^{\vee}_{d_2,S_2}$) which contradicts the $\mathcal{C}^{\vee}_{d_2,S_2}$-hiding of the scheme $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$. Hence, the claim holds. □

Proof of Claim 5 Let us assume for contradiction that there exists $b \in \{0,1\}$, a polynomial p and a distinguisher $D \in \mathcal{P}/\text{poly}$ such that for infinitely many $n \in \mathbb{N}$ D distinguishes $\mathsf{emim}^A_{H_0}(b)$ from $\mathsf{emim}^A_{H_1}(b)$ with probability $1/p(n)$.

Now, consider the set Γ of prefixes of transcripts up to the point where the first message in the left interaction is sent. By a standard averaging argument, there must exist a $1/2p(n)$ fraction of prefixes ρ in Γ, such that, conditioned on ρ occurring in both $H_0(b)$ and $H_1(b)$, the probability that D distinguishes the distributions is at least $1/2p(n)$. Fix one such prefix ρ; let h be the hash function contained in the first message in the left interaction in ρ and $s = (x_1, x_2)$ be lexicographically first collision of h. Then, using A, the prefix ρ and its collision s, we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_2,S_2}$ that violates the hiding of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$ with advantage at least $1/2p(n)$.

The circuit B is similar in spirit to the circuit described in the proof of Claim 4. B with ρ and s hard-wired in it, participates in $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$'s hiding game and internally emulates an execution of $H_1(b)$ with A as follows:

[23] For right interactions whose messages are not in ρ, B sends the first-round message by running the honest receiver $\widehat{R}$.

- Steps 1,2 and 3 are identical to the adversarial circuit described in Claim 4.
- Step 4: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_1$ on $\widetilde{c1}_i$ to obtain values $\widetilde{v}'_i$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.
- Step 5: B then runs D with the view of A and the values $\{\widetilde{v}_i'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if B receives a commitment to the random string $r1$, then it perfectly emulates $H_0(b)$ conditioned on ρ occurring for A and if it receives a commitment to the solution s which is a collision of h then it perfectly emulates $H_1(b)$ conditioned on ρ occurring for A. Moreover, for every successful interaction i, B sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ and for every unsuccessful interaction, it sets $\widetilde{v}'_i = \perp$. Therefore, the input to D (by B) is identical to $\mathsf{emim}^A_{H_0}(b)$ in the former case and it is identical to $\mathsf{emim}^A_{H_1}(b)$ in the latter case. Since D distinguishes the distributions with probability $1/2p(n)$, B wins the hiding game with advantage at least $1/2p(n)$.

Next, we argue that $B \in \mathcal{C}^{\vee}_{d_2,S_2}$: Apart from running A, B runs $o\mathcal{E}_1$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c1}_i$, and the rest of the computation takes polynomial time (includes running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, we have,

$$\begin{aligned}\mathsf{dep}(B) &= \mathsf{dep}(A) + m \cdot \mathsf{dep}(o\mathcal{E}_1) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(n) \cdot \mathsf{poly}(d_2)\\ &< \mathsf{poly}(d_2) \qquad (\text{since, } d_2 >> d_4 \text{ from Equation (9)})\end{aligned}$$

and $\mathsf{size}(B) = \mathsf{poly}(S_{\mathsf{CRH}}) < \mathsf{poly}(S^*)$. Therefore, B belongs to the circuit class C_{d_2} (resp., $B \in \mathcal{C}^{\vee}_{d_2,S_2}$) which contradicts the $\mathcal{C}^{\vee}_{d_2,S_2}$-hiding of $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$. Hence, the claim holds. □

Proof of Claim 6 Let us assume for contradiction that there exists $b \in \{0,1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ there exists a right interaction k such that k is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$, is a fake witness with probability at least $1/p(n)$. Then, using A we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_4,S_4}$ that violates the hiding of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$ with advantage at least $1/2p(n)$.

The circuit B with k hard-wired in it, participates $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$'s hiding game and internally emulates an execution of $H_2(b)$ with A as follows:

- Step 1: On receiving the first message $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ from A, B obtains the lexicographically first collision s for the hash function h via brute-force.[24]
- Step 2: It computes commitment $c2$ to the collision s. Let $d2$ be the corresponding decommitment string.
- Step 3: It samples a random string $r3$ and sends $r3$ and $(s, d2)$ (decommitment of $c2$ to s) as challenges in the hiding game of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$, and receives a commitment c^* to either $r3$ or $(s, d2)$.
- Step 4: B generates the second message of the left interaction identically to $H_2(b)$ except that it embeds c^* as the ECom_4 commitment in the message. That is, B computes $(c1, c3, b_{\mathsf{NM}})$ as in $H_2(b)$ (and $H_1(b)$) and then computes the second message of ZAP (b_{ZAP}) by setting $c4 = c^*$ and using the honest witness. It then sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message in the left interaction to A.

[24] From now onwards we will, unless specified otherwise, refer to the collision s for the hash function h in the left interaction as the lexicographically first such collision. We avoid writing it explicitly from now on.

- Step 5: Once, B receives the second round message in the kth right interaction, if the interaction is not successful then B outputs 0. Otherwise, it runs the extractor $o\mathcal{E}_{\mathsf{NM}}$ on $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$ and outputs 1 iff the extracted value is a fake witness (i.e., B outputs 1 iff the extracted value is a decommitment of $\widetilde{c4}_k$ to a decommitment of $\widetilde{c2}_k$ to a collision $\widetilde{s}_k$ of $\widetilde{h}_k$).

It is easy to see that if B receives a commitment to the random string $r3$, then it perfectly emulates $H_1(b)$ for A and if it receives a commitment to the decommitment of $c2$ to a collision s of h then it perfectly emulates $H_2(b)$ for A. By Claim 4, in the former case, the extracted value is a fake witness with only negligible probability. Therefore, B outputs 1 with negligible probability. In the latter case, by our assumption that the right interaction k is successful and the value extracted is a fake witness with probability $1/p(n)$; B outputs 1 with probability at least $1/p(n)$. Therefore, B has advantage at least $1/2p(n)$ in violating the hiding of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$.

Moreover, we show that $B \in \mathcal{C}^{\vee}_{d_4,S_4}$: B internally runs $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, $o\mathcal{E}_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{S'_{\mathsf{NM}},S'_{\mathsf{NM}}}$, finds a collision for h using a circuit in $\mathcal{C}^{\wedge}_{S'_{\mathsf{CRH}},S'_{\mathsf{CRH}}}$ the rest of the computation done by B takes $\mathsf{poly}(n)$ time. Thus, we have,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{size}(o\mathcal{E}_{\mathsf{NM}}) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(S'_{\mathsf{NM}}) + \mathsf{poly}(S'_{\mathsf{CRH}})\\ &< \mathsf{poly}(S_4) \qquad (\text{since, } S_4 >> S'_{\mathsf{NM}}, S'_{\mathsf{CRH}}, d_4 \text{ from Equation (9)})\end{aligned}$$

Therefore, B belongs to the circuit class $\mathcal{C}^{\wedge}_{S_4,S_4}$ (resp., $B \in \mathcal{C}^{\vee}_{d_4,S_4}$) which contradicts the $\mathcal{C}^{\vee}_{d_4,S_4}$-hiding of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$. Hence, the claim holds. □

Proof of Claim 7 Let us assume for contradiction that there exists $b \in \{0,1\}$, a polynomial p and a distinguisher $D \in \mathcal{P}/\text{poly}$ such that for infinitely many $n \in \mathbb{N}$ D distinguishes $\mathsf{emim}^A_{H_1}(b)$ from $\mathsf{emim}^A_{H_2}(b)$ with probability $1/p(n)$. Then using A and D, we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_4,S_4}$ that violates the hiding of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$ with non-negligible advantage $1/p(n)$. B is similar in spirit to the circuit described in the proof of Claim 6.

B participates in the hiding game of ECom_4 and internally emulates an execution of $H_2(b)$ with A as follows:

- Steps 1, 2, 3 and 4 are identical to the adversarial circuit described in Claim 6.
- Step 5: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_1$ on $\widetilde{c1}_i$ to obtain values $\widetilde{v}'_i$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.
- Step 6: B then runs D with the view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if B receives a commitment to the random string $r3$, then it perfectly emulates $H_1(b)$ for A and if it receives a commitment to the decommitment of $c2$ to a collision s of h then it perfectly emulates $H_2(b)$ for A. Moreover, for every successful interaction i, B sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ and for every unsuccessful interaction, it sets $\widetilde{v}'_i = \perp$. Therefore, the input to D (by B) is identical to $\mathsf{emim}^A_{H_1}(b)$ in the former case and it is identical to $\mathsf{emim}^A_{H_2}(b)$ in the latter case. Since D distinguishes the distributions with probability $1/p(n)$, B wins the hiding game with advantage at least $1/p(n)$.

Next, we argue that $B \in \mathcal{C}^{\vee}_{d_4,S_4}$: Apart from running A and finding a collision for h, B runs $o\mathcal{E}_1$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c1}_i$, and the rest of the computation takes polynomial time (includes

running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ and a collision for h can be found by a circuit in $\mathcal{C}^{\wedge}_{S'_{\mathsf{CRH}},S'_{\mathsf{CRH}}}$, we have,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + m \cdot \mathsf{size}(o\mathcal{E}_1) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(n) \cdot \mathsf{poly}(S_{\mathsf{CRH}}) + \mathsf{poly}(S'_{\mathsf{CRH}})\\ &< \mathsf{poly}(S_4) \qquad (\text{since, } S_4 >> S_{\mathsf{CRH}}, S'_{\mathsf{CRH}}, d_4 \text{ from Equation (9)})\end{aligned}$$

Therefore, B belongs to the circuit class C_{S_4} (resp., $B \in \mathcal{C}^{\vee}_{d_4,S_4}$) which contradicts the $\mathcal{C}^{\vee}_{d_4,S_4}$-hiding of $(\mathsf{ECom}_4, \mathsf{EOpen}_4)$. Hence, the claim holds. □

Proof of Claim 8 Let us assume for contradiction that there exists $b \in \{0,1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ there exists a right interaction k such that k is successful and the value $((\widetilde{s}'_k, \widetilde{d2}'_k), \widetilde{d4}'_k)$, extracted from $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$, is a fake witness with probability at least $1/p(n)$. Then, using A we construct a non-uniform circuit $A_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{S_{\mathsf{NM}},S_{\mathsf{NM}}}$, that participates in one left interaction with C and one right interaction with R, and a distinguisher D_{NM} that violate the one-one non-malleability of $\langle C, R\rangle$ w.r.t. extraction with advantage at least $1/2p(n)$. We detail the circuits A_{NM} and D_{NM} below.

The circuit A_{NM} with k hard-wired in it, participates in one left interaction with C and one right interaction with R and internally emulates an execution of $H_3(b)$ with A as follows:

- Step 1: A_{NM} waits for A to select identities for the left interaction with $\widehat{C}$ and the kth right interaction with $\widehat{R}$ while emulating $\widehat{R}$ for all other right interactions. Let id and $\widetilde{\mathsf{id}}_k$ be the respective identities.

- Step 2: A_{NM} selects identity $\mathsf{id}_l = \mathsf{id}$ for its left interaction and identity $\mathsf{id}_r = \widetilde{\mathsf{id}}_k$ for its right interaction r. On receiving the first-round message $a_{\mathsf{NM}r}$ from R, A_{NM} samples a hash function $\widetilde{h}_k$ and the first message of ZAP, $\widetilde{a}_{\mathsf{ZAP}k}$. It sends the tuple $(\widetilde{h}_k, \widetilde{a}_{\mathsf{NM}k} = a_{\mathsf{NM}r}, \widetilde{a}_{\mathsf{ZAP}k})$ as the first-round message to A in the kth right interaction.

- Step 3: On receiving the first message $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ from A, A_{NM} obtains a collision s for h via brute-force search.

- Step 4: A_{NM} computes commitments $(c1, c2, c3, c4)$ as in $H_3(b)$. Let $d2$ be the decommitment string of the commitment $c2$, which commits to the collison s. Furthermore, let $d4$ be the decommitment string of $c4$ which commits to a decommitment of $c2$.

- Step 5: A_{NM} samples a random string $r2$ and sends $a_{\mathsf{NM}l} = a_{\mathsf{NM}}$ as the first message to C along with the values $r2$ and $((s, d2), d4)$ as challenges and receives the second message $b_{\mathsf{NM}l}$ such that $(a_{\mathsf{NM}l}, b_{\mathsf{NM}l})$ either commit to $r2$ or $((s, d2), d4)$.

- Step 6: A_{NM} computes the second message of ZAP (b_{ZAP}) by setting $b_{\mathsf{NM}} = b_{\mathsf{NM}l}$ using the honest witness. Then, it sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message to A in the left interaction.

- Step 7: On receiving the second message $(\widetilde{c1}_k, \widetilde{c2}_k, \widetilde{c3}_k, \widetilde{c4}_k, \widetilde{b}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{ZAP}k})$ from A in the kth right interaction, B forwards $b_{\mathsf{NM}r} = \widetilde{b}_{\mathsf{NM}k}$ as the second message to R.

The distinguisher D_{NM} with input the view of A_{NM} and the value v'_r, extracted from $(a_{\mathsf{NM}r}, b_{\mathsf{NM}r})$ by $o\mathcal{E}_{\mathsf{NM}}$, runs as follows:

- D_{NM} reconstructs the entire transcript of the kth right interaction of A_{NM} with A from the view.

- If the ZAP proof $(\widetilde{a}_{\mathsf{ZAP}k}, \widetilde{b}_{\mathsf{ZAP}k})$ in the kth interaction is not accepting then D_{NM} outputs 0.

- Otherwise, D_{NM} outputs 1 iff the extracted value v'_r is such that it is a decommitment of $\widetilde{c4}_k$ to a decommitment of $\widetilde{c2}_k$ to a collision of the hash $\widetilde{h}_k$.

It is easy to see that if A_{NM} receives $b_{\mathsf{NM}l}$ such that $(a_{\mathsf{NM}l}, b_{\mathsf{NM}l})$ commit to a random string $r2$ then it perfectly emulates $H_2(v)$ for A and if $b_{\mathsf{NM}l}$ is such that $(a_{\mathsf{NM}l}, b_{\mathsf{NM}l})$ commit to $((s, d2), d4)$ then it perfectly emulates $H_3(b)$ for A. By Claim 6, in the former case, the extracted value v'_r is a fake witness with only negligible probability. Therefore, D_{NM} outputs 1 with negligible probability. In the latter case, by our assumption that the right interaction k is successful and the value extracted is a fake witness with probability $1/p(n)$; D_{NM} outputs 1 with probability at least $1/p(n)$. Therefore, D_{NM} has advantage at least $1/2p(n)$ in distinguishing the two cases, implying $(A_{\mathsf{NM}}, D_{\mathsf{NM}})$ break the one-one non-malleability w.r.t. extraction of $\langle C, R\rangle$.

Moreover, we argue that $A_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{S_{\mathsf{NM}}, S_{\mathsf{NM}}}$ and $D_{\mathsf{NM}} \in \mathcal{P}/\mathrm{poly}$: Firstly, note that $D_{\mathsf{NM}} \in \mathcal{P}/\mathrm{poly}$ as all the computation done by D_{NM} only takes polynomial time.

Next, for A_{NM}: A_{NM} internally runs $A \in \mathcal{C}^{\wedge}_{d_4, d_4}$, finds a collision for h using a circuit in $\mathcal{C}_{S'_{\mathsf{CRH}}}$ and the rest of the computation done by A_{NM} takes $\mathsf{poly}(n)$ time. Therefore, the size $\mathsf{size}(A_{\mathsf{NM}})$ of A_{NM} satisfies the following,

$$\begin{aligned}
\mathsf{size}(A_{\mathsf{NM}}) &= \mathsf{size}(A) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n) \\
&\leq \mathsf{poly}(d_4) + \mathsf{poly}(S'_{\mathsf{CRH}}) \qquad (12) \\
&< \mathsf{poly}(S_{\mathsf{NM}}) \qquad (\text{since, } S_{\mathsf{NM}} >> d_4, S'_{\mathsf{CRH}} \text{ from Equation (9)})
\end{aligned}$$

Thus, A_{NM} belongs to the circuit class $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}}, S_{\mathsf{NM}}}$ which contradicts the $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}}, S_{\mathsf{NM}}}$-one-one non-malleability w.r.t. extraction of $\langle C, R\rangle$. Hence, the claim holds. □

Proof of Claim 9 Let us assume for contradiction that there exists $b \in \{0, 1\}$, a distinguisher $D \in \mathcal{P}/\mathrm{poly}$ and a polynomial p such that D distinguishes $\mathsf{emim}^A_{H_2}(b)$ from $\mathsf{emim}^A_{H_3}(b)$ with probability $1/p(n)$. Then using A and D, we construct a non-uniform circuit $B \in \mathcal{C}^{\wedge}_{S_{\mathsf{NM}}, S_{\mathsf{NM}}}$ that violates the hiding of $\langle C, R\rangle$ with non-negligible advantage $1/p(n)$. B is similar in spirit to the circuit A_{NM} described in the proof of Claim 8.

B participates in the hiding game of $\langle C, R\rangle$ and internally emulates an execution of $H_3(b)$ with A as follows:

- Step 1: On receiving the first message $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ from A, B obtains a collision s for the hash function h via brute-force.

- Step 2: B computes commitments $(c1, c2, c3, c4)$ as in $H_3(b)$. Let $d2$ be the decommitment string of the commitment $c2$, which commits to the collision s. Furthermore, let $d4$ be the decommitment string of the commitment $c4$ to the decommitment $c2$.

- Step 3: B samples a random string $r2$ and sends a_{NM} as the first message to C along with the values $r2$ and $((s, d2), d4)$ as challenges and receives the second message b_{NM} such that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ either commit to $r2$ or $((s, d2), d4)$.

- Step 4: B computes the ZAP proof using the honest witness and sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message to A in the left interaction.

- Step 5: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_1$ on $\widetilde{c1}_i$ to extract values $\widetilde{v}'_i$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.

- Step 6: B then runs D with the view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if second message b_{NM} received by B is such that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commit to a random string $r2$, then B is perfectly emulating $H_2(b)$ for A and if b_{NM} is such that $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$ commits to $((s, d2), d4)$, then it perfectly emulating $H_3(b)$ for A. Moreover, for every successful interaction i, B sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ and for every unsuccessful interaction B sets $\widetilde{v}'_i = \perp$. Therefore, the input to D (by B) is identical to $\mathsf{emim}^A_{H_2}(b)$ in the former case and it is identical to $\mathsf{emim}^A_{H_3}(b)$ in the latter case. Since D distinguishes the distributions with probability $1/p(n)$, B wins the hiding game with advantage at least $1/p(n)$.

Next, we argue that $B \in \mathcal{C}^{\wedge}_{S_{\mathsf{NM}},S_{\mathsf{NM}}}$: Apart from running A and using a circuit in $\mathcal{C}_{S'_{\mathsf{CRH}}}$ to find the collision s, B runs $o\mathcal{E}_1$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c1}_i$, and the rest of the computation takes polynomial time (including running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, the size of B satisfies the following,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + m \cdot \mathsf{size}(o\mathcal{E}_1) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(n) \cdot \mathsf{poly}(S_{\mathsf{CRH}}) + \mathsf{poly}(S'_{\mathsf{CRH}})\\ &< \mathsf{poly}(S_{\mathsf{NM}}) \quad (\text{since, } S_{\mathsf{NM}} >> d_4, S_{\mathsf{CRH}}, S'_{\mathsf{CRH}} \text{ from Equation (9)})\end{aligned} \tag{13}$$

Therefore, B belongs to the circuit class $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}},S_{\mathsf{NM}}}$ which contradicts $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}},S_{\mathsf{NM}}}$-hiding of $\langle C, R\rangle$. Hence, the claim holds. □

Proof of Claim 10 Let us assume for contradiction that there exists $b \in \{0, 1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ there exists a right interaction k such that k is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$, is a fake witness with probability at least $1/p(n)$. Then, using A we construct a non-uniform circuit $B \in \mathcal{C}_{S^*}$ that violates the $\mathcal{C}_{S^*}$-WI of ZAP with advantage at least $1/2p(n)$.

The circuit B with k hard-wired in it, participates in the WI game of ZAP and internally emulates an execution of $H_4(b)$ with A as follows:

- Step 1: On receiving the first message $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ from A, B obtains a collision s to the hash function h. Let (v_0, v_1) be the values chosen by A for the left interaction.

- Step 2: B computes commitments $(c1, c2, c3, c4, b_{\mathsf{NM}})$ (as in $H_4(b)$). Let $d1$ be the decommitment string of the commitment $c1$, which commits to the value v_b, $d4$ be the decommitment of $c4$ which commits to $(s, d2)$ where $d2$ is the decommitment string of the commitment $c2$, which commits to the collison s. Furthermore, let $d3$ and d be the decommitments of $c3$ and $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$.

- Step 3: B sends a_{ZAP} as the first message in the WI game of ZAP with the statement $x = (h, c1, c2, c3, c4, a_{\mathsf{NM}}, b_{\mathsf{NM}})$ and witnesses $w_0 = (v_b, d1, d3)$ and $w_1 = (((s, d2), d4), d)$. B receives the second message b_{ZAP} of ZAP that is either computed by using the witness w_0 or w_1.

- Step 4: B sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second message to A on the left.

- Step 5: Once, B receives the second round message in the kth right interaction, if the interaction is not successful then B outputs 0. Otherwise, it runs the extractor $o\mathcal{E}_{\mathsf{NM}}$ on $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$ and outputs 1 iff the extracted value is a fake witness.

It is easy to see that if the second message b_{ZAP} of ZAP is computed using the witness $w_0 = (v_b, d1, d3)$ then B perfectly emulates $H_3(b)$ for A and if the second message b_{ZAP} of ZAP is computed using the witness $w_1 = (((s, d2), d4), d)$ then B perfectly emulates $H_4(b)$ for A. By Claim 8, in the former case, the extracted value is a fake witness with only negligible probability. Therefore, B outputs 1 with negligible probability. In the latter case, by our assumption that k is successful and the value extracted is a fake witness with probability $1/p(n)$; B outputs 1 with probability at least $1/p(n)$. Therefore, B has advantage at least $1/2p(n)$ in violating the WI of ZAP.

Moreover, we show that $B \in \mathcal{C}_{S^*}$: B internally runs $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, $o\mathcal{E}_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{S'_{\mathsf{NM}},S'_{\mathsf{NM}}}$, obtains a collision for h by using a circuit in $\mathcal{C}_{S'_{\mathsf{CRH}}}$ and the rest of the computation done by B takes $\mathsf{poly}(n)$ time. Thus, we have,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{size}(o\mathcal{E}_{\mathsf{NM}}) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(S'_{\mathsf{NM}})\\ &< \mathsf{poly}(S^*) \qquad (\text{since, } S^* >> d_4, S'_{\mathsf{CRH}}, S'_{\mathsf{NM}} \text{ from Equation (9)})\end{aligned}$$

Therefore, B belongs to the circuit class $\mathcal{C}_{S^*}$ which contradicts the $\mathcal{C}_{S^*}$-witness-indistinguishability of ZAP. Hence, the claim holds. □

Proof of Claim 11 Let us assume for contradiction that there exists $b \in \{0,1\}$, a polynomial p and a distinguisher D such that for infinitely many $n \in \mathbb{N}$ D distinguishes $\mathsf{emim}^A_{H_3}(b)$ from $\mathsf{emim}^A_{H_4}(b)$ with probability $\frac{1}{p(n)}$. Then using A and D, we construct a non-uniform circuit $B \in \mathcal{C}_{S^*}$ that violates the $\mathcal{C}_{S^*}$-WI of ZAP with advantage at least $1/p(n)$. B is similar in spirit to the circuit described in the proof of Claim 10.

B with participates in the WI game of ZAP and internally emulates an execution of $H_4(b)$ with A as follows:

- Steps 1,2,3 and 4 are identical to the circuit described in Claim 10.
- Step 5: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_1$ on $\widetilde{c1}_i$ to extract values $\widetilde{v}'_i$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.
- Step 6: B then runs D with the view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if the second message b_{ZAP} of ZAP is computed using the witness $w_0 = (v_b, d1, d3)$ then B perfectly emulates $H_3(b)$ for A and if the second message b_{ZAP} of ZAP is computed using the witness $w_1 = (((s, d2), d4), d)$ then B perfectly emulates $H_4(b)$ for A. Moreover, for every successful interaction i, B sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ and for every unsuccessful interaction, it sets $\widetilde{v}'_i = \perp$. Therefore, the input to D (by B) is identical to $\mathsf{emim}^A_{H_3}(b)$ in the former case and it is identical to $\mathsf{emim}^A_{H_4}(b)$ in the latter case. Since D distinguishes the distributions with probability $1/p(n)$, B wins the hiding game with advantage at least $1/p(n)$.

Next, we argue that $B \in \mathcal{C}_{S^*}$: Apart from running A and finding a collision for h, B runs $o\mathcal{E}_1$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c1}_i$, and the rest of the computation takes polynomial time (includes running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, we have,

$$\begin{aligned}\mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{poly}(S'_{\mathsf{CRH}}) + m \cdot \mathsf{size}(o\mathcal{E}_1) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n) \cdot \mathsf{poly}(S_{\mathsf{CRH}})\\ &< \mathsf{poly}(S^*) \qquad (\text{since, } S^* >> d_4, S_{\mathsf{CRH}}, S'_{\mathsf{CRH}} \text{ from Equation (9)})\end{aligned}$$

Therefore, B belongs to the circuit class $\mathcal{C}_{S^*}$ which contradicts the $\mathcal{C}_{S^*}$-WI of ZAP. Hence, the claim holds. □

Proof of Claim 12 Let us assume for contradiction that there exists $b \in \{0,1\}$ and a polynomial p such that for infinitely many $n \in \mathbb{N}$ there exists a right interaction k such that k is successful and the value extracted from $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$, is a fake witness with probability at least $1/p(n)$. Then, using A we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_3,S_3}$ that violates the hiding of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ with advantage at least $1/2p(n)$.

The circuit B with k hard-wired in it, participates in $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$'s hiding game, and internally emulates an execution of $H_5(b)$ with A as follows:

- Step 1: On receiving the first message $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ from A, B obtains a collison s to the hash function h. Let (v_0, v_1) be the values chosen by A for the left interaction.
- Step 2: It computes $(c1, c2, c4, b_{\mathsf{NM}})$ as in $H_5(b)$. Let $d1$ be the decommitment string of the commitment $c1$ which is a commitment to v_b.
- Step 3: Then in the hiding game of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$, B sends $(v_b, d1)$ and 0^l as challenges and receives a commitment c^* to either $(v_b, d1)$ or 0^l.
- Step 4: B generates the second message of ZAP (b_{ZAP}) by setting $c3 = c^*$. It then sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message in the left interaction to A.
- Step 5: Once, B receives the second round message in the kth right interaction, if the interaction is not successful then B outputs 0. Otherwise, it runs the extractor $o\mathcal{E}_{\mathsf{NM}}$ on $(\widetilde{a}_{\mathsf{NM}k}, \widetilde{b}_{\mathsf{NM}k})$ and outputs 1 iff the extracted value is a fake witness.

It is easy to see that if B receives a commitment to $(v_b, d1)$, then it perfectly emulates $H_4(b)$ for A and if it receives a commitment to 0^l then it perfectly emulates $H_5(b)$ for A. By Claim 10, in the former case, the extracted value is a fake witness with only negligible probability. Therefore, B outputs 1 with negligible probability. In the latter case, by our assumption that the right interaction k is successful and the value extracted is a fake witness with probability $1/p(n)$; B outputs 1 with probability at least $1/p(n)$. Therefore, B has advantage at least $1/2p(n)$ in violating the hiding of ECom_3.

Next, we argue that $B \in \mathcal{C}^{\vee}_{d_3,S_3}$: B internally runs $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, $o\mathcal{E}_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{S'_{\mathsf{NM}},S'_{\mathsf{NM}}}$, obtains a collision for h using a circuit in $\mathcal{C}_{S'_{\mathsf{CRH}}}$ and the rest of the computation done by B takes $\mathsf{poly}(n)$ time. Thus, we have,

$$\begin{aligned}
\mathsf{size}(B) &= \mathsf{size}(A) + \mathsf{size}(o\mathcal{E}_{\mathsf{NM}}) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n) \\
&\leq \mathsf{poly}(d_4) + \mathsf{poly}(S'_{\mathsf{NM}}) + \mathsf{poly}(S'_{\mathsf{CRH}}) \\
&< \mathsf{poly}(S_3) \qquad (\text{since, } S_3 >> d_4, S'_{\mathsf{NM}}, S'_{\mathsf{CRH}} \text{ from Equation (9)})
\end{aligned}$$

Therefore, B belongs to the circuit class $\mathcal{C}^{\wedge}_{S_3,S_3}$ (resp., $B \in \mathcal{C}^{\vee}_{d_3,S_3}$) which contradicts the $\mathcal{C}^{\vee}_{d_3,S_3}$-hiding of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$. Hence, the claim holds. □

Proof of Claim 13 Let us assume for contradiction that there exists $b \in \{0,1\}$, a polynomial p and a distinguisher $D \in \mathcal{P}/\text{poly}$ such that for infinitely many $n \in \mathbb{N}$ D distinguishes $\mathsf{emim}^A_{H_4}(b)$ from $\mathsf{emim}^A_{H_5}(b)$ with probability $1/p(n)$. Then using A and D, we construct a non-uniform circuit $B \in \mathcal{C}^{\vee}_{d_3,S_3}$ that violates the hiding of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ with non-negligible advantage $1/p(n)$. B is similar in spirit to the circuit described in the proof of Claim 10.

B participates in the hiding game of the scheme $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ and internally emulates an execution of $H_5(b)$ with A as follows:

- Steps 1-4 are identical to the adversarial circuit described in Claim 12.

- Step 5: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_1$ on $\widetilde{c1}_i$ to extract values $\widetilde{v}'_i$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.

- Step 6: B then runs D with the view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if B receives a commitment to $(v_b, d1)$, then it perfectly emulates $H_4(b)$ for A and if it receives a commitment to 0^l then it perfectly emulates $H_5(b)$ for A. Moreover, B for every successful interaction i, sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ and for every unsuccessful interaction, it sets $\widetilde{v}'_i = \perp$. Therefore, the input to D (by B) is identical to $\mathsf{emim}^A_{H_4}(b)$ in the former case and it is identical to $\mathsf{emim}^A_{H_5}(b)$ in the latter case. Since D distinguishes the distributions with probability $1/p(n)$, B wins the hiding game with advantage at least $1/p(n)$.

Next, we argue that $B \in \mathcal{C}^{\vee}_{d_3,S_3}$: Apart from running A and finding a collision for h using a circuit in $\mathcal{C}_{S'_{\mathsf{CRH}}}$, B runs $o\mathcal{E}_1$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c1}_i$, and the rest of the computation takes polynomial time (includes running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, we have,

$$\begin{aligned}
\mathsf{size}(B) &= \mathsf{size}(A) + m \cdot \mathsf{size}(o\mathcal{E}_1) + \mathsf{poly}(S'_{\mathsf{CRH}}) + \mathsf{poly}(n) \\
&\leq \mathsf{poly}(d_4) + \mathsf{poly}(n) \cdot \mathsf{poly}(S_{\mathsf{CRH}}) + \mathsf{poly}(S'_{\mathsf{CRH}}) \\
&< \mathsf{poly}(S_3) \qquad (\text{since, } S_3 >> S_{\mathsf{CRH}}, d_4, S'_{\mathsf{CRH}} \text{ from Equation (9)})
\end{aligned}$$

Therefore, B belongs to the circuit class $\mathcal{C}_{S_3}$ (resp., $B \in \mathcal{C}^{\vee}_{d_3,S_3}$) which contradicts the $\mathcal{C}^{\vee}_{d_3,S_3}$-hiding of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$. Hence, the claim holds. □

Proof of Claim 15 Let us assume for contradiction that there exists $b \in \{0,1\}$, a polynomial p and a distinguisher $D \in \mathcal{P}/\text{poly}$ such that for infinitely many $n \in \mathbb{N}$ D distinguishes $\mathsf{emim}^A_{H_5}(b)$ from $\mathsf{emim}^A_{H_6}(b)$ with probability $1/p(n)$.

Now, consider the set Γ of prefixes of transcripts up to the point where the first message in the left interaction is sent. By a standard averaging argument, there must exist a $1/2p(n)$ fraction of prefixes ρ in Γ, such that, conditioned on ρ occurring in both $H_5(b)$ and $H_6(b)$, the probability that D distinguishes the distributions is at least $1/2p(n)$. Fix one such prefix ρ; let h be the hash function contained in the first message in the left interaction in ρ and $s = (x_1, x_2)$ be the lexicographically first collision of h. Then, using A, the prefix ρ and its collision s, we construct a non-uniform circuit $B \in \mathcal{C}_{d_1}$ that violates the hiding of $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ with advantage at least $1/3p(n)$.

B with ρ and s hard-wired in it, participates in $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$'s hiding game and internally emulates an execution of $H_6(b)$ with A as follows:

- Step 1: Feed A with messages in ρ; let $(h, a_{\mathsf{ZAP}}, a_{\mathsf{NM}})$ be the left first message. Let (v_0, v_1) be the values sent by A in the left interaction.

- Step 2: B sends v_b and v_0 as challenges in the hiding game of the scheme $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ and receives a commitment c^* to either v_b or v_0.

- Step 3: B generates the second message of the left interaction identically to $H_6(b)$ except that it embeds c^* as the ECom_1 commitment in the message. That is, B computes $(c2, c3, c4, b_{\mathsf{NM}})$ as in $H_6(b)$ (using the collision s received as non-uniform advice) and then computes the second message of ZAP (b_{ZAP}) by setting $c1 = c^*$. It then sends $(c1, c2, c3, c4, b_{\mathsf{NM}}, b_{\mathsf{ZAP}})$ as the second round message in the left interaction to A.

- Step 4: After A terminates, for every successful right interaction i, B runs the extractor $o\mathcal{E}_3$ on $\widetilde{c3}_i$ to extract values $(\widetilde{v}'_i, \widetilde{d1}'_i)$. For every unsuccessful right interaction i, B sets $\widetilde{v}'_i = \perp$.
- Step 4: B then runs D with the view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$ as inputs, and returns the output of D as its output.

It is easy to see that if B receives a commitment to v_b, then it perfectly emulates $H_5(b)$ conditioned on ρ occurring for A and if it receives a commitment to v_0 then it perfectly emulates $H_6(b)$ conditioned on ρ occurring for A. Moreover, for every successful interaction i, B sets $\widetilde{v}'_i$ to the value extracted by $o\mathcal{E}_3$ from $\widetilde{c3}_i$ and for every unsuccessful interaction, it sets $\widetilde{v}'_i = \perp$. We claim that the input to D (by B) is statistically close to $\mathsf{emim}^A_{H_5}(b)$ in the former case and it is statistically close to $\mathsf{emim}^A_{H_6}(b)$ in the latter case; the proof of claim is presented shortly. Since D distinguishes $\mathsf{emim}^A_{H_5}(b)$ from $\mathsf{emim}^A_{H_5}(b)$ with probability $1/2p(n)$, we conclude that B wins the hiding game with advantage at least $1/3p(n)$.

Next, we argue that $B \in \mathcal{C}_{d_1}$: Apart from running A, B runs $o\mathcal{E}_3$ on $m = \mathsf{poly}(n)$ commitments $\widetilde{c3}_i$, and the rest of the computation takes polynomial time (includes running D). Since, $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and $o\mathcal{E}_3 \in \mathcal{C}^{\wedge}_{d_1,S_4}$,

$$\begin{aligned}\mathsf{dep}(B) &= \mathsf{dep}(A) + m \cdot \mathsf{dep}(o\mathcal{E}_3) + \mathsf{poly}(n)\\ &\leq \mathsf{poly}(d_4) + \mathsf{poly}(n) \cdot \mathsf{poly}(d_1)\\ &< \mathsf{poly}(d_1) \qquad (\text{since, } d_1 >> d_4 \text{ from Equation (9)})\end{aligned}$$

Furthermore, $\mathsf{size}(B) < \mathsf{poly}(S^*)$. Therefore, B belongs to the circuit class $\mathcal{C}_{d_1}$ (resp., $B \in \mathcal{C}^{\vee}_{d_1,S_1}$) which contradicts the $\mathcal{C}^{\vee}_{d_1,S_1}$-hiding of $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$.

It remains to show our claim that the input to distinguisher D by adversary B (i.e., view of A and the values $\{\widetilde{v_i}'\}_{i\in[m]}$) is indeed (1) statistically close to $\mathsf{emim}^A_{H_5}(b)$ when B receives a commitment to v_b and (2) statistically close to $\mathsf{emim}^A_{H_6}(0)$ when it receives a commitment to v_0. We will argue (1) and the proof of (2) follows similarly. Recall that for every successful right interaction i, B runs $o\mathcal{E}_3$ on $\widetilde{c3}_i$ to obtain $(\widetilde{v}'_i, \widetilde{d1}'_i)$. We claim that the value $\widetilde{v}'_i$ is identical to the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$, except with negligible probability. Since i is successful, by Claim 14 we know that with overwhelming probability the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is not a fake witness with overwhelming probability. Then by the over-extractability $\langle C, R\rangle$ we know that the value committed in $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is not a fake witness. Furthermore, due to soundness of ZAP, it must be that with overwhelming probability the commitments $\widetilde{c1}_i$ and $\widetilde{c3}_i$ are valid and $\widetilde{c3}_i$ commits to a decommitment of $\widetilde{c1}_i$. Then, by the over-extractability of $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ the value $(\widetilde{v}'_i, \widetilde{d1}'_i)$ extracted from $\widetilde{c3}_i$ is identical to $\mathsf{val}(\widetilde{c3}_i)$ with over-whelming probability, where $\mathsf{val}(\widetilde{c3}_i)$ is a decommitment of $\widetilde{c1}_i$ — $(\widetilde{v}_i, \widetilde{d1}_i)$. Next, due to the over-extractability of ECom_1, the value extracted by $o\mathcal{E}_1$ from $\widetilde{c1}_i$ is identical to $\mathsf{val}(\widetilde{c1}_i) = \widetilde{v}_i$ with overwhelming probability. Therefore, the value $\widetilde{v}_i$ obtained by B is identical to the value that $o\mathcal{E}_1$ extracts from $\widetilde{c1}_i$ with overwhelming probability. This is now sufficient to conclude that the input to D is statistically close to $\mathsf{emim}^A_{H_5}(b)$ when B receives a commitment to v_b except with negligible probability. This establishes (1) and (2) follows by the same argument. Hence the claim holds. □

7 Amplifying Length of Identities – Log n trick

The Non-malleability strengthening technique (Section 6.3) applied to the scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ of Section 5, that supports identities of length $t(n) = O(1)$, results in a concurrent non-malleable

commitment scheme but still only supports identities of length $t(n) = O(1)$. However, our final goal is to construct a scheme that supports identities of length n. In this section, we provide a transformation that amplifies the length of identities exponentially.

Given a tag-based commitment scheme $\langle \widehat{C}, \widehat{R} \rangle$ for $t(n)$-bit identities which is concurrent non-malleable w.r.t. commitment, Dolev, Dwork and Naor [DDN00] construct a tag-based commitment scheme $\langle \widetilde{C}, \widetilde{R} \rangle$ for exponentially larger identities, namely identities of length $2^{t(n)-1}$-bits. In their work [DDN00], they show that their transformation results in a commitment scheme that can accomodate significantly larger length of identities but degrades concurrent non-malleability w.r.t. commitment to stand-alone non-malleability w.r.t. commitment. Furthermore, their reduction also incurs a polynomial security loss.

The commitment schemes considered in this work are non-malleable w.r.t. extraction and we claim that their transformation also works for such schemes. That is, we show that if $\langle \widehat{C}, \widehat{R} \rangle$ is concurrent non-malleable w.r.t. extraction then commitment scheme $\langle \widetilde{C}, \widetilde{R} \rangle$ is standalone non-malleable w.r.t. extraction. The key idea towards amplifying the length of identities is embedding a $2^{t(n)-1}$-bit identity into $2^{t(n)-1}$ number of $t(n)$-bit identities — we, thereby, refer to this idea as the "log-n" trick. The protocol from [DDN00] is based on the log-n trick and is described below.

The committer $\widetilde{C}$ and receiver $\widetilde{R}$ receive the security parameter 1^n and identity $\mathsf{id} \in \{0,1\}^{t'(n)}$ as common input where $t'(n) = 2^{t(n)-1}$. Furthermore, $\widetilde{C}$ gets a private input $v \in \{0,1\}^\alpha$ which is the value to be committed.

- *Commit stage:*

  1. To commit to a value $v \in \{0,1\}^\alpha$, $\widetilde{C}$ chooses t' random shares $r_0, r_1, \ldots, r_{t'-1} \in \{0,1\}^\alpha$ such that $v = r_0 \oplus r_1 \oplus \ldots \oplus r_{t'-1}$.
  2. For each $0 \leq i \leq t'-1$, $\widetilde{C}$ and $\widetilde{R}$ run $\langle \widehat{C}, \widehat{R} \rangle$ to commit to r_i (in parallel) using identity $(i, \mathsf{id}[i])$ where $\mathsf{id}[i]$ is the ith bit of id. Let d_i be the corresponding decommitment string.

  Let c_i be the transcript of $\langle \widehat{C}, \widehat{R} \rangle$ committing to r_i with identity $(i, \mathsf{id}[i])$. Then we denote by $c = \{c_i\}_{0 \leq i \leq t'-1}$ the entire transcript of the interaction.

- *Reveal stage:*
  On receiving the decommitment $(v, \{r_i\}_i, \{d_i\}_i)$, $\widetilde{R}$ verifies (1) for each $0 \leq i \leq t'-1$, c_i is a commitment to r_i using $\langle \widehat{C}, \widehat{R} \rangle$ and identity $(i, \mathsf{id}[i])$, and (2) $v = r_0 \oplus r_1 \oplus \ldots \oplus r_{t'-1}$. $\widetilde{R}$ accepts the decommitment iff (1) and (2) hold.

Furthermore, let us assume that $\langle \widehat{C}, \widehat{R} \rangle$ is over-extractable w.r.t. extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ then we construct an extractor $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ for $\langle \widetilde{C}, \widetilde{R} \rangle$ as follows,

- Extraction - Algorithm $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$:
  On receiving $\mathsf{id} \in \{0,1\}^{t'}$ and commitment $c = \{c_i\}_{0 \leq i \leq t'-1}$, $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ runs $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ on each c_i obtaining output r'_i. If any of the r'_i is $\perp$ then $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ outputs $\perp$. Otherwise, it outputs $v' = r'_0 \oplus r'_2 \oplus \ldots \oplus r'_{t'-1}$ as the extracted value.

Theorem 16 (Log-n trick [DDN00])**.** *Let t be such that $t'(n) = 2^{t(n)-1}$ is a polynomial. Let $\langle \widehat{C}, \widehat{R} \rangle$ be a commitment scheme and $\mathcal{C}$ be a class of circuits that is closed under composition with $\mathcal{P}$/poly.*

1. *If $\langle \widehat{C}, \widehat{R} \rangle$ is a tag based perfectly binding commitment scheme for $t(n)$-bit identities then $\langle \widetilde{C}, \widetilde{R} \rangle$ is a tag based perfectly binding commitment scheme for identities of length $t'(n) = 2^{t(n)-1}$ bits.*

2. *If* $\langle \widehat{C}, \widehat{R} \rangle$ *is concurrent* $\mathcal{C}$*-non-malleable w.r.t. commitment then* $\langle \widetilde{C}, \widetilde{R} \rangle$ *is one-one* $\mathcal{C}$*-non-malleable w.r.t. commitment.*

3. *If* $\langle \widehat{C}, \widehat{R} \rangle$ *is* (d, S)*-over-extractable by* $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ *then* $\langle \widetilde{C}, \widetilde{R} \rangle$ *is* (d, S)*-over-extractable by* $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$*. Furthermore, if* $\langle \widehat{C}, \widehat{R} \rangle$ *is concurrent* $\mathcal{C}$*-non-malleable w.r.t. extraction by* $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ *then* $\langle \widetilde{C}, \widetilde{R} \rangle$ *is standalone* $\mathcal{C}$*-non-malleable w.r.t. extraction by* $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$*.*

Proof. We prove each of the above in the following:

- Perfect binding and tag lengths: The perfect binding of $\langle \widetilde{C}, \widetilde{R} \rangle$ follows from the statistical binding of $\langle \widehat{C}, \widehat{R} \rangle$. Furthermore, $\langle \widetilde{C}, \widetilde{R} \rangle$ as defined above accomodates identities of length $t' = 2^{t(n)-1}$-bits.

- Non-malleability w.r.t. extraction: Assume for contradiction that there exists a non-uniform attacker $A = \{A_n\}_{n \in \mathbb{N}} \in \mathcal{C}$ that participates in one left with $\widetilde{C}$ and one right interaction with $\widetilde{R}$ sending/receiving commitments to values of length $\alpha = \mathsf{poly}(n)$-bits, a non-uniform distinguisher $D = \{D_n\}_{n \in \mathbb{N}} \in \mathcal{P}/\text{poly}$ and a polynomial $p(\cdot)$ such that for infinitely many $n \in \mathbb{N}$,

$$\left| \mathsf{Pr}[D_n(\mathsf{emim}^{A_n}_{\langle \widetilde{C}, \widetilde{R} \rangle}(1^n, 0)) = 1] - \mathsf{Pr}[D_n(\mathsf{emim}^{A_n}_{\langle \widetilde{C}, \widetilde{R} \rangle}(1^n, 1)) = 1] \right| \geq 1/p(n) \ ,$$

  where $\mathsf{emim}^{A}_{\langle \widetilde{C}, \widetilde{R} \rangle}(1^n, b)$ describes the view of A, and value $\tilde{v}'$ extracted from the right commitment $\widetilde{c} = \{\widetilde{c}_i\}_{0 \leq i \leq t'-1}$ by extractor $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$. Recall that $\tilde{v}'$ is set to $\perp$ when $\mathsf{id} = \tilde{\mathsf{id}}$ for A's choice of left and right identities id and $\tilde{\mathsf{id}}$ respectively. When $\mathsf{id} \neq \tilde{\mathsf{id}}$, by the definition of extractor $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$, $\tilde{v}' = \tilde{v}'_0 \oplus \ldots \oplus \tilde{v}'_{t'-1}$ where $\tilde{v}'_i$ are the values extracted from $\tilde{c}_i$ by extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$.

  Next, we construct a one-many non-uniform adversary $A' = \{A'_n\}_{n \in \mathbb{N}}$, and a non-uniform distinguisher $D' = \{D'_n\}_{n \in \mathbb{N}}$ such that for infinitely many $n \in \mathbb{N}$

$$\left| \mathsf{Pr}[D'_n(\mathsf{emim}^{A'}_{\langle \widehat{C}, \widehat{R} \rangle}(1^n, 0)) = 1] - \mathsf{Pr}[D'_n(\mathsf{emim}^{A'}_{\langle \widehat{C}, \widehat{R} \rangle}(1^n, 1)) = 1] \right| \geq 1/(p(n) \cdot t').$$

  The adversary A' internally runs A, participates in one left interaction with $\widehat{C}$ and $m = t'(n)$ right interactions with $\widehat{R}$ and internally emulates an execution of $\mathsf{IND}^{A}_{\langle \widetilde{C}, \widetilde{R} \rangle}(b)$ for A as follows:

  - Step 1: For the right interaction with A, A' emulates the honest receiver $\widetilde{R}$ using its $t'(n)$ right interactions with $\widehat{R}$, by simply forwarding messages between A and $\widehat{R}$. A' waits for A to select identity for its left interaction. Let id be the $t'(n)$-bit identity and v_0, v_1 be the values sent by A for the left interaction. Let $\mathsf{s}_i = (i, \mathsf{id}[i])$ for $0 \leq i \leq t' - 1$.
  - Step 2: To continue with the left interaction, A' samples a random $j \leftarrow_{\$} \{0, \ldots, t' - 1\}$. Let $I = \{0, \ldots, t' - 1\} \setminus \{j\}$. A' samples random shares $r_i \leftarrow_{\$} \{0,1\}^{\alpha}$ for $i \in I$ and sets $u_b = v_b \oplus r$ where $r = \oplus_{i \in I}\ r_i$. Then, A' begins its left interaction with $\widehat{C}$ with identity $\mathsf{s} = \mathsf{s}_j$ and challenges values u_0, u_1.
  - Step 3: A' interacts with A acting as a honest committer $\widetilde{C}$ to compute the commitment $c = \{c_i\}_{0 \leq i \leq t'-1}$. More precisely, for all $i \in I$, A acts as the honest committer $\widehat{C}$ to generate the commitment c_i to value r_i under identity s_i. The commitment c_j is the commitment to value u_b under identity $\mathsf{s} = \mathsf{s}_j$ generated by forwarding messages between A and the external committer $\widehat{C}$. It is easy to see that if $\widehat{C}$ commits to u_b then c is a commitment to v_b under $\langle \widetilde{C}, \widetilde{R} \rangle$ with identity id.

The distinguisher D' with input the view of A' and the values $(\tilde{v}'_1, \ldots, \tilde{v}'_{t'})$ extracted by extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ from the t' right commitments of A', runs as follows:

- Step 1: D' reconstructs the view of A in emulation by A'. Furthermore, let id,$\tilde{\mathsf{id}}$ be the identities chosen by A for its left and right interactions (defined by the view of A) respectively and let $\mathsf{s} = (j, \mathsf{id}[j])$ be the identity chosen by A' for some $0 \leq j \leq t' - 1$. And let $\tilde{\mathsf{s}}_i = (i, \tilde{\mathsf{id}}[i])$ for all $0 \leq i \leq t' - 1$.
- Step 2: If $\mathsf{id} \neq \tilde{\mathsf{id}}$ but $\mathsf{s} = \tilde{\mathsf{s}}_j$ for some $j \in \{0, \ldots, t' - 1\}$ then D' aborts.[25] Otherwise, D' sets $\tilde{v}' = \oplus_{0 \leq i \leq t'-1}\ v'_i$.
- Step 2: D' then runs D on the above reconstructed view of A and $\tilde{v}'$ and returns whatever D' returns.

First, observe that whenever $\widehat{C}$ commits to u_b, A' perfectly simulates the MIM experiment $\mathsf{MIM}^{A}_{\langle \widehat{C}, \widehat{R} \rangle}(b)$ for A. Conditioned on D' not aborting, we know that A' choice of left identity s is distinct from all right identities $\tilde{\mathsf{s}}_j$. Therefore, by definition of $\mathsf{emim}^{A'}_{\langle \widehat{C}, \widehat{R} \rangle}$, D''s inputs $\tilde{v}'_i$ are the values extracted by the extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ from the i-th right commitment $\tilde{c}_i$. Therefore, the value $\tilde{v}'$ reconstructed by D' is identical to the value extracted by $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ from A's right commitment $\tilde{c} = \{\tilde{c}_i\}_{0 \leq i \leq t'-1}$. Therefore, conditioned on not aborting, D' perfectly reconstructs $\mathsf{emim}^{A}_{\langle \widetilde{C}, \widetilde{R} \rangle}(b)$ from its input $\mathsf{emim}^{A'}_{\langle \widehat{C}, \widehat{R} \rangle}(b)$. Since D distinguishes $\mathsf{emim}^{A}_{\langle \widetilde{C}, \widetilde{R} \rangle}(0)$ from $\mathsf{emim}^{A}_{\langle \widetilde{C}, \widetilde{R} \rangle}(1)$ with advantage at least $1/p(n)$ and D' does not abort with probability $1/t'(n)$, we have (A', D') break the one-many non-malleability w.r.t. extraction of $\langle \widehat{C}, \widehat{R} \rangle$ with advantage $1/p(n) \cdot t'(n)$. Furthermore, note that A' internally runs A and the rest of the computation takes $\mathsf{poly}(n)$-time. Also, D' internally runs D and the rest of its computation also takes $\mathsf{poly}(n)$-time. Therefore, since $A \in \mathcal{C}$ and $\mathcal{C}$ is closed under composition with $\mathcal{P}/\mathrm{poly}$, we have $A' \in \mathcal{C}$. Also, $D \in \mathcal{P}/\mathrm{poly}$ implies that $D' \in \mathcal{P}/\mathrm{poly}$. This contradicts the one-many non-malleability of $\langle \widehat{C}, \widehat{R} \rangle$ w.r.t. extraction by $\widehat{o\mathcal{E}}_{\mathsf{NM}}$.

Remark 9. *We note that the $1/t'$ loss in the advantage of the reduction can be avoided if A sends the identity of the right interaction $\tilde{\mathsf{id}}$ before sending id. In this case, whenenver $\mathsf{id} \neq \tilde{\mathsf{id}}$ there exists at least one index $0 \leq j \leq t' - 1$ such that $\mathsf{id}[j] \neq \tilde{\mathsf{id}}[j]$ and hence $\mathsf{s}_j = (j, \mathsf{id}[j])$ is distinct from all $\tilde{\mathsf{s}}_i = (i, \tilde{\mathsf{id}}[i])$. This ensures D' never aborts. However, since we allow our MIM adversary A total control over the scheduling of messages (even choosing identities), given the left identity id we can only guess the special index j thereby inccurring a $1/t'$ loss in the advantage where $t' = |\mathsf{id}|$.*

- Non-malleability w.r.t. commitment: This follows syntactically from the same proof as Non-malleability w.r.t. extraction by replacing emim random variables with their respective mim random variables. We skip the formal proof.

- Over-extractability: A valid commitment $c = \{c_i\}_{0 \leq i \leq t'-1}$ is such that every c_i is a valid commitment for $\langle \widehat{C}, \widehat{R} \rangle$. Due to the over-extractability of $\langle \widehat{C}, \widehat{R} \rangle$ w.r.t. $\widehat{o\mathcal{E}}_{\mathsf{NM}}$, for every $0 \leq i \leq t' - 1$, the extractor $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ always extracts the correct value r'_i. Therefore, $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ always extracts the correct value from c. Since, t' is a polynomial, $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ fails with negligible probability. Moreover, $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$ runs $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ on t' commitments and rest of the computation

[25] This is because, the value $\tilde{v}'_j$ given as input to D' will be replaced with $\perp$ disallowing D' to reconstruct the input to D.

takes $\mathsf{poly}(n)$ time. Therefore, if $\widehat{o\mathcal{E}}_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{d,S}$ then $\widetilde{o\mathcal{E}}_{\mathsf{NM}} \in \mathcal{C}^{\wedge}_{d,S}$. Therefore, $\langle \tilde{C}, \tilde{R} \rangle$ is (d, S)-over-extractable w.r.t. $\widetilde{o\mathcal{E}}_{\mathsf{NM}}$.

□

8 Concurrent Non-malleable Commitment for n-bit Identities

In this section, we construct a concurrent non-malleable commitment scheme $\langle C^*, R^* \rangle$ that can accomodate n-bit identities. This then concludes the proof of Theorem 1 (formally stated in Theorem 17). The idea is to start with the basic commitment scheme from Section 5 that is one-one non-malleable w.r.t. extraction for short identities, say $t(n)$-bits. Then apply the non-malleability strengthening technique described in Section 6.3 followed by the log-n trick [DDN00] described in Section 7 repeatedly until the length of the identities reaches n-bits. The resulting commitment scheme is the commitment scheme $\langle C^*, R^* \rangle$. We detail the construction of $\langle C^*, R^* \rangle$ more formally in Section 8.1, provide instantiations in Section 8.2, discuss the efficiency of the scheme $\langle C^*, R^* \rangle$ in Section 8.3 and argue about the security $\langle C^*, R^* \rangle$ in Section 8.4.

Theorem 17. *For some sub-exponential functions T, B assume the existence of $\mathcal{C}^{\wedge}_{B,B}$-secure injective one-way functions, $\mathcal{C}^{\wedge}_{B,B}$-WI ZAP, $\mathcal{C}^{\wedge}_{B,B}$-collison-resistant hash function family and (T, B)-secure Time-lock puzzles. Then, $\langle C^*, R^* \rangle$ is a 2-round, perfectly binding concurrent non-malleable w.r.t. extraction and w.r.t. commitment against poly-size adversaries.*

8.1 Commitment Scheme $\langle C^*, R^* \rangle$

We formally describe the construction of $\langle C^*, R^* \rangle$ that is concurrent non-malleable w.r.t. commitment (and extraction) for n-bit identities. As mentioned above we initially start with a commitment scheme $\langle C^0, R^0 \rangle$ for $t(n)$-bit identities and apply the non-malleability strengthening and log-n trick repeatedly, for say $r(n)$ times, until we reach identities of length n-bits.

- Initial Scheme $\langle C^0, R^0 \rangle$:
  The initial scheme $\langle C^0, R^0 \rangle$ is the basic scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$, as constructed in Section 5, that is one-one non-malleable w.r.t. extraction for identities of length $\mathsf{id}^0(n) = t(n)$-bits. Furthermore, let $\langle C^0, R^0 \rangle$ be non-malleable against circuits of depth at most $\mathsf{poly}(S^0)$ and size at most $\mathsf{poly}(S^0)$ and extractable by an extractor of depth $\mathsf{poly}(S'^0)$ and size $\mathsf{poly}(S'^0)$.[26]

- Identity Amplification Step for $r(n)$ Times:
  Next, we repeatedly apply the following two steps $r(n)$ number of times. Let $\langle C^{j-1}, R^{j-1} \rangle$ be the commitment scheme at the end of the $j-1$-st iteration for $j \in [r(n)]$. We describe below the j-th iteration below. Let $\langle C^{j-1}, R^{j-1} \rangle$ be one-one non-malleable w.r.t. commitment (and extraction) for identities of length $\mathsf{id}^{j-1}(n)$-bits. Furthermore, let $\langle C^{j-1}, R^{j-1} \rangle$ be non-malleable against circuits of depth at most $\mathsf{poly}(S^{j-1})$ and size at most $\mathsf{poly}(S^{j-1})$ and extractable by an extractor of depth $\mathsf{poly}(S'^{j-1})$ and size $\mathsf{poly}(S'^{j-1})$.

[26] Note that the initial scheme as presented in Section 5 is non-malleable against circuits of depth at most $\mathsf{poly}(d_0)$ and size at most $\mathsf{poly}(S_0)$ where $d_0 << S_0$. However, note that such a scheme is still non-malleable against circuits of depth at most $\mathsf{poly}(d_0)$ and size at most $\mathsf{poly}(d_0)$.

1. Non-malleability Strengthening Technique:
   First, using an appropriate hierarchy of functions as described in Eq (9), we apply the non-malleability strengthening technique to the scheme $\langle C^{j-1}, R^{j-1}\rangle$ to boost its one-one non-malleability to concurrent non-malleability. The resulting scheme $\langle \widehat{C}^j, \widehat{R}^j\rangle$ is concurrent non-malleable w.r.t. commitment (and extraction) for identities of length $\mathsf{id}^{j-1}(n)$-bits.
2. Log-n Trick:
   Second, we apply the log-n trick to the concurrent non-malleable scheme $\langle \widehat{C}^j, \widehat{R}^j\rangle$ to construct a one-one non-malleable commitment $\langle C^j, R^j\rangle$ for identities of length $\mathsf{id}^j(n)$ such that $\mathsf{id}^j(n) = 2^{\mathsf{id}^{j-1}(n)-1}$.

- Final Scheme $\langle C^*, R^*\rangle$:
  The commitment scheme $\langle C^{r(n)}, R^{r(n)}\rangle$ constructed at the end of $r(n)$ iterations is one-one non-malleable for identities of length $\mathsf{id}^{r(n)}$. We apply the non-malleability strengthening technique one more time to $\langle C^{r(n)}, R^{r(n)}\rangle$ to boost its one-one non-malleability to concurrent non-malleability. The resulting scheme $\langle C^*, R^*\rangle$ is concurrent non-malleable for identities of length $\mathsf{id}^{r(n)}(n)$-bits.

Note that we begin we identities of length $\mathsf{id}^0 = t(n)$ and identities in successive iterations satisfy the following,

$$\mathsf{id}^j(n) = 2^{\mathsf{id}^{j-1}(n)-1} .$$

Then it is easy to see that for $\mathsf{id}^{r(n)}(n) \geq n$ and $t(n) > 2$, we need to apply the identity amplification step $r(n) = O(\log^* n - \log^* t(n))$ times.

8.2 Instantiations

The initial scheme constructed in Section 5 and the identity amplification step described in Sections 6.3,7 require a family of depth-robust and size-robust commitment schemes, and a family of non-uniform collision resistant hash functions which are based on some hierarchy of non-decreasing functions. Below we detail the size of this hierarchy required for constructing $\langle C^*, R^*\rangle$ from the initial scheme $\langle C^0, R^0\rangle$ for $t(n)$-bit identities and $r(n)$ iterations of the identity amplification step. Then we give instantiations of this hierarchy firstly from sub-exponential security and then from the strictly weaker sub-subexponential security.

Initial Scheme $\langle C^0, R^0\rangle$. We start with the basic scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ for $t(n)$-bit identities. As described in Section 5, the construction of the scheme $(\mathsf{ENMCom}, \mathsf{ENMOpen})$ for $t(n)$-bit identities requires a family of $2^{t(n)}$ size-robust and depth-robust commitment schemes w.r.t. the following hierarchy of non-decreasing functions,

$$n << d_0 << d_1 << \ldots << d_{l-1} << d_l << S_0 << S_1 << \ldots << S_{l-1} << S_l ,$$

where $l = 2^{t(n)}$ such that for every $i \in \{0,1\}^{t(n)}$,

- there exists a depth-robust commitment scheme $(\mathsf{ECom}_{d_i}, \mathsf{EOpen}_{d_i})$ that is $\mathcal{C}_{d_i}$-hiding and (d_{i+1}, d_{i+1})-over-extractable w.r.t. an extractor $o\mathcal{E}_{d_i}$.
- there exists a size-robust commitment scheme $(\mathsf{ECom}_{S_i}, \mathsf{EOpen}_{S_i})$ that is $\mathcal{C}^{\wedge}_{S_i,S_i}$-hiding and $(\mathsf{poly}(n), S_{i+1})$-over-extractable w.r.t. an extractor $o\mathcal{E}_{S_i}$.

Therefore, to construct the initial commitment scheme we need a hierarchy of $2(l+1) = 2(2^{t(n)}+1)$ non-decreasing functions.

Identity Amplification Step. Consider the $j+1$-st iteration of the identity amplification step described in the construction of $\langle C^*, R^* \rangle$. In the $j+1$-st iteration, we are applying the strengthening technique to the commitment scheme $\langle C^j, R^j \rangle$ which is $\mathcal{C}^{\wedge}_{S^j, S^j}$-non-malleable and extractable by a circuit of size $\mathsf{poly}(S'^j)$. The strengthening technique requries a family of four depth-robust [27] and four size-robust commitment schemes. Furthermore, it also requires a family of non-uniform collision-resistant hash functions w.r.t. the following hierarchy of non-decreasing functions,

$$\begin{aligned} &n << d_4^j << d_3^j << d_1^j << d_2^j << S_2^j << S_1^j << S_{\mathsf{CRH}}^j << \\ &S_{\mathsf{CRH}}'^j << S^j << S'^j << S_3^j << S_4^j << S_4'^j << S^* \ , \end{aligned} \tag{14}$$

such that,

- $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_1^j, S_1^j}$-hiding and $(d_2^j, S_{\mathsf{CRH}}^j)$-over-extractable w.r.t. extractor $o\mathcal{E}_1$.
- $(\mathsf{ECom}_2, \mathsf{EOpen}_2)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_2^j, S_2^j}$-hiding and (S_2^j, S_1^j)-over-extractable w.r.t. extractor $o\mathcal{E}_2$.
- $(\mathsf{ECom}_3, \mathsf{EOpen}_3)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_3^j, S_3^j}$-hiding and $(d_1^j, S_4'^j)$-over-extractable w.r.t. extractor $o\mathcal{E}_3$.
- $(\mathsf{ECom}_4, \mathsf{ECom}_4)$ is a perfectly binding commitment scheme which is $\mathcal{C}^{\vee}_{d_4^j, S_4^j}$-hiding and $(d_3^j, S_4'^j)$-over-extractable w.r.t. extractor $o\mathcal{E}_4$.
- $\mathcal{H} = \{H_n\}_{n \in \mathbb{N}}$ is a $\mathcal{C}^{\wedge}_{S_{\mathsf{CRH}}^j, S_{\mathsf{CRH}}^j}$ -collision-resistant family of hash functions such that a collision can be found by a circuit of size $\mathsf{poly}(S_{\mathsf{CRH}}'^j)$.

Furthermore, we apply the log-n trick to the resulting commitment scheme. Note that the log-n trick does not rely on any additional tools. Therefore, in an iteration of the identity amplification step, we need four depth-robust[27], four size-robust commitment schemes and a hash function family. In other words, we need an additional at most eleven[28] non-decreasing functions per iteration. Therefore, over $r(n)$ iterations, we will need a hierarchy of $11r(n)+11$ functions.[29]

Therefore, to construct the commitment scheme $\langle C^*, R^* \rangle$ from $\langle C^0, R^0 \rangle$ for $t(n)$-bit identities, we need a hierarchy of $L = 2^{t(n)+1} + 11r(n) + 13$ non-decreasing functions, where $r(n) = O(\log^* n - \log^* t(n))$. Furthermore, L is minimized when $t(n) = O(1)$, implying $r(n) = O(\log^* n)$ and $L = O(\log^* n)$. Next, we show two approaches to instantiate a hierarchy of $L = O(\log^* n)$ non-decreasing functions, one from sub-exponential security and another from sub-subexponential security.

[27] Note that the transformation actually requires four depth-and-size robust commitment schemes but as described in Section 4.3 depth-and-size robust commitment scheme can be constructed from a single depth-robust and a size-robust commitment scheme.

[28] nine levels are required for the four depth-and size-robust commitment schemes (see Equation 14) namely $d_1, \ldots, d_4$, $S_1, \ldots, S_4, S_4'$ and additional two levels namely S_{CRH} and S_{CRH}' for the collision-resistant hash function.

[29] The additional eleven functions is due an extra application of the non-malleability strengthening to boost the non-malleability of $\langle C^{r(n)}, R^{r(n)} \rangle$.

Instantiation from Sub-exponential Security. As mentioned above, we need to instantiate a hierarchy of L non-decreasing functions for constructing $\langle C^*, R^* \rangle$. Let the required hierarchy be the following,

$$p_1 << p_2 << \ldots << p_L \ . \tag{15}$$

Let $\mathcal{F}(\lambda)$ be some non-decreasing, invertible function defined on $\mathbb{N}$ such that $\mathcal{F}(\lambda) = \omega(\log \lambda)$ but $\mathcal{F}(\lambda) = o(\lambda)$. It is easy to see that $\mathcal{F}(\lambda) = \lambda^{\varepsilon}$ satisfies the requirements for any $0 < \varepsilon < 1$. First we will instantiate the hierarchy (Equation 15) based on the existence of $2^{\mathcal{F}(\lambda)}$-secure primitives and then provide concrete parameters for the special case of sub-exponential security, that is, for $\mathcal{F}(\lambda) = \lambda^{\varepsilon}$ for some $\varepsilon < 1$.

Towards this, first assume the existence of $(T(t) = 2^{\mathcal{F}(t)}, B(n) = 2^{\mathcal{F}(n)})$-secure TL puzzle, $2^{\mathcal{F}(k)}$-secure injective OWF, $2^{\mathcal{F}(\theta)}$-collision-resistant hash family where $(n, t), k, \theta$ are security parameters for the underlying TL puzzle, injective OWF and collision-resistant hash respectively. We instantiate the above hierarchy, that is, p_1 through p_L from $2^{\mathcal{F}(\lambda)}$-security by varying the security parameter λ. Let n be the security parameter of the non-malleable commitment scheme we want to construct. Then, consider the following sequence of security parameters

$$n_0 \ , n_1 \ , \ldots \ , n_L \ ,$$

where each n_i is some function of n (we specify these shortly). We set i-th level (i.e., p_i) in the required hierarchy as,

$$p_i = 2^{\mathcal{F}(n_i)} \ .$$

We expect the functions in the hierarchy to satisfy certain constraints in order for us to be able to instantiate the required depth-robust, size-robust commitment schemes, and collision-resistant hash function from them. We list the properties below.

1. Since we expect all our primitives to be secure against any poly-sized circuit, we require that the first security parameter n_0 be such that $2^{\mathcal{F}(n_0)} \geq 2^{\omega(\log n)}$ that is,

$$\mathcal{F}(n_0) = \omega(\log n) \ ,$$
$$n_0 = \mathcal{F}^{-1}(\omega(\log n)) \ .$$

2. For any i, we need to be able to instantiate the following primitives,

   (a) (p_i, p_{i+1})-depth-robust commitment scheme: Commitment scheme that is $\mathcal{C}p_i$-hiding but (p_{i+1}, p_{i+1})-over-extractable. We instantiate such a scheme from TL puzzles with security parameter $t(n) = n_i(n)$.[30] Then by the $2^{\mathcal{F}(t)}$-security of TL puzzles combined with $t(n) = n_i(n)$ (or equivalently $2^{\mathcal{F}(t)} = 2^{\mathcal{F}(n_i)} = p_i$), the resulting puzzles are hard for adversaries in $\mathcal{C}p_i$. To guarantee that the puzzles can be solved by some circuit of size $\mathsf{poly}(p_{i+1})$, we require that

   $$2^{t(n)} = 2^{n_i(n)} \leq p_{i+1} \ . \tag{16}$$

   If Equation 16 holds then by Theorem 8, we have a (p_i, p_{i+1})-depth-robust-commitment scheme.

[30] Recall that TL puzzles have two security parameters n and t. The security parameter n is the security parameter of the non-malleable commitment scheme. Therefore, we sample puzzles from the support of $\mathsf{Gen}(1^n, 1^{n_i}, \cdot)$ in the depth-robust commitment scheme in Section 4.1.

(b) (p_i, p_{i+1})-size-robust commitment scheme: A commitment scheme that is $\mathcal{C}^{\wedge}_{p_i,p_i}$-hiding but $(\mathsf{poly}(n), p_{i+1})$-over-extractable. We instantiate such a scheme from $2^{\mathcal{F}(k)}$-secure injective OWF on input-length $k(n) = n_i(n)$. Then, the $2^{\mathcal{F}(k)}$-security guarantees that the resulting OWF (one with security parameter $k = n_i$) is hard to invert for adversaries in $\mathcal{C}^{\wedge}_{p_i,p_i}$. Furthermore, such a function can be inverted by a circuit of size $\mathsf{poly}(n_i) \cdot 2^{n_i}$ and depth $\mathsf{poly}(n_i)$. Therefore, to guarantee that function can be inverted by a circuit of size $\mathcal{C}^{\wedge}_{\mathsf{poly}(n),p_{i+1}}$, we require that,

$$n_i \leq \mathsf{poly}(n) \quad ; \quad 2^{n_i} \leq p_{i+1} \ . \tag{17}$$

If Equation 17 holds then by Theorem 9, we have a (p_i, p_{i+1})-size-robust-commitment scheme.

(c) (p_i, p_{i+1})-collision-resistant hash function family: A (p_i, p_{i+1})-collision-resistant hash function family is a family of hash functions that is $\mathcal{C}^{\wedge}_{p_i,p_i}$-collision resistant and for which there exists a circuit of size $\mathsf{poly}(p_{i+1})$ that finds collisions with probability 1. We instantiate such a family by setting the security parameter θ of $\mathcal{H}$ as $\theta(n) = n_i(n)$, where $\mathcal{H}$ is a family of $2^{\mathcal{F}(\theta)}$-collision-resistant hash functions. As discussed above, the $2^{\mathcal{F}(\theta)}$-collision resistance of $\mathcal{H}$ implies that the resulting function is $\mathcal{C}^{\wedge}_{p_i,p_i}$-collision resistant. To guarantee that a circuit of size $\mathsf{poly}(p_{i+1})$ finds collisions, we require that

$$2^{n_i} \leq p_{i+1} \ . \tag{18}$$

Setting $n_{i+1} = \mathcal{F}^{-1}(n_i)$ implies $p_{i+1} = 2^{\mathcal{F}(n_{i+1})} = 2^{n_i}$ which guarantees that Equations 16, 17, 18 hold. This entails a sequence $n_1, \ldots, n_L$ where the i-th security parameter n_i is,

$$n_i = \left(\mathcal{F}^{-1}\right)^{i+1} (\omega(\log n)) \ .$$

3. Finally we require that the last security parameter n_L be upper-bounded by some $\mathsf{poly}(n)$,

$$n_L = \left(\mathcal{F}^{-1}\right)^{L+1} (\omega(\log n)) \leq \mathsf{poly}(n) \ . \tag{19}$$

Now let us consider the case of sub-exponential security, that is, let $\mathcal{F} = \lambda^{\varepsilon}$ for some $0 < \varepsilon < 1/2$. Then, $\mathcal{F}^{-1}(y) = y^{1/\varepsilon}$ be the inverse of $\mathcal{F}$. For the last security level n_L to be polynomially bounded, we require that,

$$(\omega(\log n))^{(1/\varepsilon)^{L+1}} \leq \mathsf{poly}(n) \ .$$

It is easy to see that from subexponential security, we can derive $L = \Theta(\log \log n)$ levels. Recall that to construct $\langle C^*, R^* \rangle$ we need $O(\log^* n)$ levels in the hierarchy, hence the above hierarchy finds an instantiation from subexponential security.

However, for our transformation, we require only $L = O(\log^* n)$ levels which is significantly less than $\Theta(\log \log n)$ levels that can be extracted from sub-exponential security. Hence, there is hope to instantiate the hierarchy from weaker than sub-exponential security. In fact, such a hierarchy can, indeed, be instantiated from strictly weaker security — *sub-subexponential* security — which we show below.

Instantiation from Sub-subexponential Security. First we define the notion of sub-subexponential security and then provide an instantiation of the hierarchy. Informally, a $2^{\mathcal{F}(\lambda)}$-secure primitive is sub-subexponential -secure if

$$\mathcal{F}(\lambda) \in \lambda^{o(1)} \ .$$

A candidate for $\mathcal{F}$ for sub-subexponential security is the following,

$$\mathcal{F}(\lambda) = \lambda^{\frac{1}{\mathcal{X}(\lambda)}} \ ,$$

where $\mathcal{X}(\lambda) = \omega(1)$ be some non-decreasing function on $\mathbb{N}$.

We ask how large (if at all) such an $\mathcal{X}(\lambda) = \omega(1)$ can be so that we can still instantiate the above hierarchy. The only point of concern is bounding the security parameter n_L of the last level, that is, we ask how large $\mathcal{X}(\lambda)$ be such that for $\mathcal{F}(\lambda) = \lambda^{\frac{1}{\mathcal{X}(\lambda)}}$ and $L = O(\log^* n)$ the following holds,

$$n_L = \left(\mathcal{F}^{-1}\right)^L (\omega(\log n)) \leq \mathsf{poly}(n) \ .$$

However the above closed form is hard to analyse so we restrict the right hand side to be n instead of a generic $\mathsf{poly}(n)$, that is,

$$\left(\mathcal{F}^{-1}\right)^L (\omega(\log n)) \leq n \tag{20}$$

Applying $\mathcal{F}$ on both sides we get,

$$\left(\mathcal{F}^{-1}\right)^{L-1} (\omega(\log n)) \leq \mathcal{F}(n) \ , \tag{21}$$

Let $n' = \mathcal{F}(n) = n^{\frac{1}{\mathcal{X}(n)}} < n$. We have,

$$\mathcal{F}(n') = \left(n'\right)^{\frac{1}{\mathcal{X}(n')}} = \left(\mathcal{F}(n)\right)^{\frac{1}{\mathcal{X}(n')}} \ .$$

Since $\mathcal{X}$ is a non-decreasing function we have,

$$\mathcal{F}(n') = \left(\mathcal{F}(n)\right)^{\frac{1}{\mathcal{X}(n')}} > \left(\mathcal{F}(n)\right)^{\frac{1}{\mathcal{X}(n)}} \ , \tag{22}$$

Applying again $\mathcal{F}$ on both sides of Equation (21),

$$\left(\mathcal{F}^{-1}\right)^{L-2} (\omega(\log n)) \leq \mathcal{F}(n') \ , \tag{23}$$

Therefore by Equation (22) we know that as long as the following holds, Equation (23) holds.

$$\left(\mathcal{F}^{-1}\right)^{L-2} (\omega(\log n)) \leq \mathcal{F}(n)^{\frac{1}{\mathcal{X}(n)}} = n^{\frac{1}{\mathcal{X}(n)}^2} \ .$$

After repeatedly applying $\mathcal{F}$, it is easy to see that as long as the following holds, Equation (20) holds.

$$\omega(\log n) \leq n^{\frac{1}{\mathcal{X}(n)^L}} \ .$$

Furthermore, the if the following holds then the above Equation holds,

$$\mathcal{X}(n)^L \leq \frac{\log n}{\omega(\log \log n)}$$

$$\mathcal{X}(n) \leq \left(\frac{\log n}{\omega(\log\log n)}\right)^{\frac{1}{O(\log^* n)}}$$

Finally, as long as the following holds for some $c > 0$ then Equation (20) holds.

$$\mathcal{X}(n) \leq (\log^c n)^{\frac{1}{O(\log^* n)}}$$

$$\mathcal{X}(n) \leq (\log n)^{\frac{1}{\Theta(\log^* n)}} \tag{24}$$

For $\mathcal{X}(n) = \log\log n$, it is easy to see that Equation (24) holds and hence Equation (20) holds. Therefore we can instantiate the above hierarchy from $2^{n^{\frac{1}{\log\log n}}}$-secure OWPs, TL puzzles and CRHs which is strictly weaker than assuming 2^{n^ε}-security.

8.3 Efficiency of $\langle C^*, R^*\rangle$

As described in Section 8.1, to construct the scheme $\langle C^*, R^*\rangle$ we apply the identity amplification step — non-malleability strengthening technique followed by the log-n trick — $O(\log^* n)$ times. Suppose that the identity amplification step incurrs a polynomial overhead, that is, on input a scheme with computational complexity $\tau(n)$, it outputs a scheme with computational complexity $p(\tau(n))$ for some fixed polynomial p. Applying this step for a super-constant number of times leads to a scheme $\langle C^*, R^*\rangle$ with super-polynomial computational complexity.

Unfortunately, our non-malleability strengthening technique presented in Section 6 indeed incurrs polynomial overhead. Recall that on input a non-malleable commitment $\langle C, R\rangle$, the technique produces an output scheme $\langle \widehat{C}, \widehat{R}\rangle$ which uses ZAP to prove a statement that involves verifying the decommitment to a commitment of $\langle C, R\rangle$. Therefore, if the decommiment function $\mathsf{Open}(c, v, d)$ of $\langle C, R\rangle$ has complexity $\tau_{\mathsf{Open}}(n)$, the output scheme has complexity at least $p_{\mathsf{ZAP}}(\tau_{\mathsf{Open}}(n))$, where p_{ZAP} is the polynomial overhead induced by ZAP.

We show below that a simple modification can fix the problem. (We chose to present the strengthening technique in simpler terms earlier for ease of exposition.) Towards this, we introduce a new property called *open-decomposability* for commtiment schemes. We say that a scheme $\langle C, R\rangle$ is g-open-decomposable, if it is the case that, its decommitment function $\mathsf{Open}(c, v, d)$ can be decomposed into two functions of the following form:

- a "public" function $\mathsf{PubOpen}(c)$ that can be verified without the decommitment (v, d), and
- a "private" function $\mathsf{PrivOpen}(c^*, v, d)$ that depends on the decommitment and only a small part $c^* = \pi(c)$ of the commitment c, and takes polynomial time $g(n)$.

Open accepts iff both $\mathsf{PubOpen}$ and $\mathsf{PrivOpen}$ accept. Consider applying the non-malleability strengthening technique on such a g-open-decomposable commitment scheme. Instead of using ZAP to verify whether Open accepts, it is equivalent to verify whether $\mathsf{PubOpen}$ accepts in the clear (outside ZAP) and only verifies whether $\mathsf{PrivOpen}$ accepts using ZAP. This simple change reduces the overhead induced by the ZAP proof from $p_{\mathsf{ZAP}}(\tau_{\mathsf{Open}}(n))$ to $p_{\mathsf{ZAP}}(g(n))$. Our key observation is that the initial non-malleable schemes, as well as all intermediate schemes produced throughout the iterations, are all open-decomposable w.r.t. small polynomials. Based on this, we can show that the complexity of the final scheme is polynomially bounded.

Open-decomposability. We formally define the notion of open-decomposability below.

Definition 20 (g-open-decomposability)**.** *Let g be a polynomial. We say that a commitment scheme $\langle C, R\rangle$ is g-open-decomposable if there exist efficiently computable functions* PubOpen*,* PrivOpen*, and π, such that, for all $n \in \mathbb{N}$, $c \in \{0,1\}^{m(n)}$, $v \in \{0,1\}^{\alpha(n)}$, $d \in \{0,1\}^{l(n)}$ and $c^* = \pi(c)$,*

$$(\mathsf{Open}(c, v, d) = 1 \iff \mathsf{PubOpen}(c) = 1) \ \wedge \ (\mathsf{PrivOpen}(c^*, v, d) = 1)\,,$$

where PrivOpen *runs in time $g(n)$. Above, $m(n)$ and $l(n)$ are respectively the maximal lengths of commitments and decommitments generated using $\langle C, R\rangle$ for values of length $\alpha(n)$ with security parameter n.*

Using the above notion, we next describe the modified non-malleability strengthening technique and log-n trick. We analyze the open-decomposability property of the schemes produced by iteratively applying these two transformations to the initial schemes constructed in Section 5, and show that the growth of the complexity of these schemes is polynomially bounded.

More specifically, let g be a sufficiently large polynomial that, in particular, is larger than the complexity of all depth-and-size robust commtiment schemes, ECom's, used for constructing the initial schemes and in the transformations. By the analysis in Section 8.2, all the ECom's used have polynomial complexity. This implies that the initial non-malleable commitment schemes (consisting of invokation of two ECom schemes) does satisfy g-open-decomposability (by simply setting PubOpen to the constant function outputting 1 and PrivOpen = Open itself). Then, we show that the non-malleability stengthening technique always outputs a scheme that is g-open-decomposable, and on input such a scheme, the log-n trick produces a scheme that is $h(n)$-open-decomposable for $h(n) = ng(n)$.

Modification to the strengthening technique described in Section 6.3. Let $\langle C, R\rangle$ be one-one non-malleable w.r.t. extraction and satisfy h-open-decomposable w.r.t. $(\mathsf{PubOpen}, \mathsf{PrivOpen}, \pi)$. We describe the changes (highlighted in red) to the non-malleability strengthening technique.

- Commit stage - First round: Same as before.
- Commit stage - Second round: Steps 1, 2 and 4 are same as before.

  3. Given a_{ZAP} and for $c^* = \pi(a_{\mathsf{NM}}, b_{\mathsf{NM}})$, $\widehat{C}$ computes the second message b_{ZAP} of ZAP to prove the following OR-statement:
     (a) *either* there exists a string $\bar{v}$ such that $c1$ is a commitment to $\bar{v}$ and $c3$ commits to a decommitment of $c1$.
     (b) *or* there exists a string $\bar{s} = (x_1, x_2)$, such that,
        – $h(x_1) = h(x_2)$,
        – $c2$ is a commitment to $\bar{s}$,
        – $c4$ commits to a decommitment of $c2$,
        – PrivOpen accepts $(c^*, d4, v4)$, and $(d4, v4)$ is a valid decommitment to $c4$.

     $\widehat{C}$ proves the statement (a) by using a decommitment of $c3$ to $(v, d1)$ — decommitment of $c1$ to v — as the witness.

  Denote by $(\hat{a}_{\mathsf{NM}}, \hat{b}_{\mathsf{NM}})$ the produced commitment.

- Reveal stage - Function $\widehat{\mathsf{Open}}((\hat{a}_{\mathsf{NM}}, \hat{b}_{\mathsf{NM}})), d1, v)$:
  Parse $(\hat{a}_{\mathsf{NM}}, \hat{b}_{\mathsf{NM}})$ and let $(a_{\mathsf{ZAP}}, b_{\mathsf{ZAP}})$, $(a_{\mathsf{NM}}, b_{\mathsf{NM}})$, and $c1$ be the ZAP proof, the commitment of $\langle C, R\rangle$, and the ECom_1 commitment contained in it. Accept if and only if the following functions both accept.
  - $\widehat{\mathsf{PubOpen}}(\hat{a}_{\mathsf{NM}}, \hat{b}_{\mathsf{NM}})$ accepts iff the ZAP proof $(a_{\mathsf{ZAP}}, b_{\mathsf{ZAP}})$ is accepting and $\mathsf{PubOpen}((a_{\mathsf{NM}}, b_{\mathsf{NM}})) = 1$.
  - $\widehat{\pi}(\hat{a}_{\mathsf{NM}}, \hat{b}_{\mathsf{NM}}) = c1$ and $\widehat{\mathsf{PrivOpen}}(c1, v, d1)$ accepts iff $\mathsf{EOpen}_1(c1, v, d1) = 1$.

The scheme $\langle \widehat{C}, \widehat{R}\rangle$ is open-decomposable w.r.t. $(\widehat{\mathsf{PubOpen}}, \widehat{\mathsf{PrivOpen}}, \widehat{\pi})$. Since $\widehat{\mathsf{PrivOpen}}$ only checks the decommitment of the ECom_1 commitment, its runtime is bounded by $g(n)$. Thus, $\langle \widehat{C}, \widehat{R}\rangle$ is $g(n)$-open-decomposable. On the other hand, since $\mathsf{PrivOpen}$ has complexity $h(n)$, the ZAP proof incurrs an additive $\mathsf{poly}(n, g(n), h(n))$ overhead. Then,

$$\widehat{cc}(n) = cc(n) + \mathsf{poly}(n, g(n), h(n)) \ ,$$

where $cc(n)$ and $\widehat{cc}(n)$ are the computational complexities of $\langle C, R\rangle$ and $\langle \widehat{C}, \widehat{R}\rangle$ respectively.

Modification to log-n trick described in Section 7. Let $\langle \widehat{C}, \widehat{R}\rangle$ be concurrent non-malleable (w.r.t. commitment and extraction) for $l(n)$-bit identities, and be $g(n)$-open-decomposable w.r.t. $(\widehat{\mathsf{PubOpen}}, \widehat{\mathsf{PrivOpen}}, \widehat{\pi})$. The log-n trick results in a commitment scheme $\langle \widetilde{C}, \widetilde{R}\rangle$ which is one-one non-malleable (w.r.t. commitment and extraction) for identities of length $l'(n) = 2^{l(n)-1} < n$. We show that $\langle \widetilde{C}, \widetilde{R}\rangle$ is $h(n)$-open-decomposable w.r.t. $(\widetilde{\mathsf{PubOpen}}, \widetilde{\mathsf{PrivOpen}}, \widetilde{\pi})$ described below.

- Commit stage: Same as before.
  Let $\widetilde{a}_{\mathsf{NM}}, \widetilde{b}_{\mathsf{NM}}$ be the produced commitment, which contains l' commitments of $\langle \widehat{C}, \widehat{R}\rangle$, denoted as $\left\{\widehat{a}^i_{\mathsf{NM}}, \widehat{b}^i_{\mathsf{NM}}\right\}_{i\in[l']}$.
- Reveal stage - Function $\widetilde{\mathsf{Open}}((\tilde{a}_{\mathsf{NM}}, \tilde{b}_{\mathsf{NM}})), d, v)$: Accept if and only if the following functions both accept.
  - $\widetilde{\mathsf{PubOpen}}$ accepts iff for every i, $\widehat{\mathsf{PubOpen}}(\widehat{a}^i_{\mathsf{NM}}, \widehat{b}^i_{\mathsf{NM}})$ accepts.
  - $\widetilde{\pi}(\widetilde{a}_{\mathsf{NM}}, \widetilde{b}_{\mathsf{NM}}) = \left\{c^*_i = \widehat{\pi}(\widehat{a}^i_{\mathsf{NM}}, \widehat{b}^i_{\mathsf{NM}})\right\}_i$ and $\widetilde{\mathsf{PrivOpen}}$ accepts iff for every i, $\widehat{\mathsf{PrivOpen}}$ accpets c^*_i w.r.t. d, v.

Note that the running time of $\widetilde{\mathsf{PrivOpen}}$ is at most $l'(n) \cdot g(n) \leq h(n)$, and hence $\langle \widetilde{C}, \widetilde{R}\rangle$ is $h(n)$-open-decomposable. Furthermore, if the computational complexity of $\langle \widehat{C}, \widehat{R}\rangle$ is $\widehat{cc}(n)$, the computational complexity of $\langle \widetilde{C}, \widetilde{R}\rangle$ is bounded by $l'(n)\widehat{cc}(n)$.

Putting Pieces Together. Every iteration, say the j'th iteration, starts with a commitment scheme $\langle C^j, R^j\rangle$ supporting $\mathsf{id}^j(n)$ length identities, that is $h(n)$-open-decomposable (the inital schemes are g-open-decomposable). Applying the non-malleability strengthening technique produces a scheme $\langle \widehat{C}^j, \widehat{R}^j\rangle$ that is $g(n)$-open-decomposable. Following that, the log-n trick produces a scheme $\langle C^{j+1}, R^{j+1}\rangle$, supporting $\mathsf{id}^{j+1}(n) = 2^{\mathsf{id}^j(n)-1}$ length identities, that is $h(n)$-open-decomposable for $h(n) = ng(n)$. Furthermore, Let $cc(j)$ denote the computational complexity of

the scheme $\langle C^j, R^j \rangle$. Then we have:

$$\begin{aligned} cc(j+1) &= \mathsf{id}^{j+1}(n)\left(cc(j) + \mathsf{poly}(n, g(n), h(n))\right) \\ &= \mathsf{id}^{j+1}(n)\left(\mathsf{id}^{j}(n)(cc(j-1) + \mathsf{poly}(n)) + \mathsf{poly}(n)\right) \\ &\leq \mathsf{id}^{j+1}(n)\mathsf{id}^{j}(n)cc(j-1) + \mathsf{id}^{j+1}(n)\mathsf{id}^{j}(n)\mathsf{poly}(n) + \mathsf{id}^{j+1}(n)\mathsf{poly}(n) \end{aligned}$$

Then,

$$\begin{aligned} cc(j+1) &\leq \mathsf{id}^{j+1}(n)\mathsf{id}^{j}(n)cc(j-1) + 2\mathsf{id}^{j+1}(n)\mathsf{id}^{j}(n)\mathsf{poly}(n) \\ &\leq \prod_{1\leq k\leq j+1} \mathsf{id}^{k}(n)cc(0) + (j+1)\left(\prod_{1\leq k\leq j+1} \mathsf{id}^{k}(n)\right)\mathsf{poly}(n) \end{aligned}$$

Since the total number of iterations is $O(\log^* n)$ and the lengths of identities grow exponentially fast, we have that the running time of the final scheme $\langle C^*, R^* \rangle$ is upper-bounded by a polynomial.

8.4 Security of $\langle C^*, R^* \rangle$

Recall from Section 8.1 $\langle C^*, R^* \rangle$ is the commitment scheme obtained by applying the non-malleability strengthening step to the commitment scheme $\langle C^{r(n)}, R^{r(n)} \rangle$ which inturn was constructed by recursively applying, for $r(n)$ iterations, the non-malleability strengthening step followed by the log-n trick starting from the basic commitment scheme $\langle C^0, R^0 \rangle$. Since, the number of iterations $r(n) = O(\log^* n)$ (i.e., $r(n) = w(1)$)[31], it is not apriori clear whether $\langle C^*, R^* \rangle$ is concurrent non-malleable for poly-size adversaries. Towards establishing the security of $\langle C^*, R^* \rangle$, we first focus on showing $\langle C^{r(n)}, R^{r(n)} \rangle$ is one-one non-malleable against poly-size adversaries. Then the security of $\langle C^*, R^* \rangle$ would follow from Theorem 13.

Recall the j-th step of the iteration: Starting from $\langle C^j, R^j \rangle$ commitment scheme on $\mathsf{id}^j(n)$-bit identities, first the non-malleability strengthening step is applied to $\langle C^j, R^j \rangle$ resulting in a scheme $\langle \widehat{C}^{j+1}, \widehat{R}^{j+1} \rangle$ on $\mathsf{id}^j(n)$-bit identities. Then, the logn trick applied to $\langle \widehat{C}^{j+1}, \widehat{R}^{j+1} \rangle$ resulting in the commitment scheme $\langle C^{j+1}, R^{j+1} \rangle$ on $\mathsf{id}^{j+1}(n)$-bit identities. By Theorems 13, 16 we know that if $\langle C^j, R^j \rangle$ is one-one non-malleable then $\langle C^{j+1}, R^{j+1} \rangle$. First, let us establish some notation for the "advantage" of a certain adversary in breaking the non-malleability of the intermediate commitment schemes.

NOTATION For $j \in [r(n)]$ consider the commitment scheme $\langle C^j, R^j \rangle$. Consider some (A, D) where $A \in \mathcal{C}^{\wedge}_{S^j, S^j}$ and $D \in \mathcal{P}/\text{poly}$ let $\varepsilon^j_{A,D}(n)$ be a function $\mathbb{N} \to [0, 1]$ such that for all $n \in \mathbb{N}$,

$$\varepsilon^j_{A,D}(n) = |\mathsf{Pr}[D_n(\mathsf{emim}^A_{\langle C^j, R^j \rangle}(1^n, 0))] - D_n(\mathsf{emim}^A_{\langle C^j, R^j \rangle}(1^n, 1))| \ .$$

Let $\varepsilon^j_A(n)$ be the maximum of $\varepsilon^j_{A,D}(n)$ over all $D \in \mathcal{P}/\text{poly}$. We refer to $\varepsilon^j_A(n)$ as A's advantage in breaking one-one non-malleability w.r.t. extraction of $\langle C^{j+1}, R^{j+1} \rangle$. Furthermore, let $\varepsilon^j(n)$ be the maximum of $\varepsilon^j_A(n)$ over all one-one adversary $A \in \mathcal{C}^{\wedge}_{S^j, S^j}$. Similarly, we define such an advantage function for the commitment scheme $\langle \widehat{C}^j, \widehat{R}^j \rangle$: For $A \in \mathcal{C}^{\wedge}_{S^j, S^j}$ participating in one left interaction with $\widehat{C}^j$ and $m^j(n) = \mathsf{id}^j(n)$ right interactions with $\widehat{R}^j$, let $\hat{\varepsilon}^j_A(n)$ be the advantage of A in breaking the one-many non-malleability of $\langle \widehat{C}^j, \widehat{R}^j \rangle$.

[31] Both non-malleability strengthening (Theorem 13) and log-n trick (Theorem 16) incur $O(m) = \mathsf{poly}(n)$ loss in the security where m is the number of concurrent interactions A participates in. Applying the transformation $r(n) = O(1)$ would have trivially implied security of $\langle C^*, R^* \rangle$.

We are interested in showing that $\varepsilon^{r(n)}(n)$ is negligible. That is, the scheme $\langle C^{r(n)}, R^{r(n)}\rangle$ is $\mathcal{C}^{\wedge}_{S^{r(n)},S^{r(n)}}$-one-one non-malleable commitment scheme on $\mathsf{id}^{r(n)}(n) \geq n$-bit identites. Since $\mathcal{P}/\text{poly} \subseteq \mathcal{C}^{\wedge}_{S^{r(n)},S^{r(n)}}$, this also establishes the security of $\langle C^{r(n)}, R^{r(n)}\rangle$ against poly-size adversaries. Towards bounding $\varepsilon^{r}(n)$, we first bound $\varepsilon^{j+1}(n)$ as a function of $\varepsilon^{j}(n)$.

First, recall that by Theorem 16, for any $A \in \mathcal{C}^{\wedge}_{S^{j+1},S^{j+1}}$ that breaks the one-one non-malleability of $\langle C^{j+1}, R^{j+1}\rangle$ with probability δ, there exists $A' \in \mathcal{C}^{\wedge}_{S^{j+1},S^{j+1}}$ that participates in one left and $\mathsf{id}^{j+1}(n)$ right interactions and breaks the one-many non-malleability of $\langle \widehat{C}^{j+1}, \widehat{R}^{j+1}\rangle$ with probability δ' such that

$$\delta \leq \mathsf{id}^{j+1}(n) \cdot \delta' \ . \tag{25}$$

Therefore, we can upperbound $\varepsilon^{j+1}(n)$ by,

$$\varepsilon^{j+1}(n) \leq \mathsf{id}^{j+1}(n) \cdot \hat{\varepsilon}^{j+1}(n) \ , \tag{26}$$

Next, recall that in the proof of Theorem 13, we reduce to the security of primitives inccuring a multiplicative loss in the advantage proportional to m – number of right interactions that the one-many adversary takes part in. While relating $\hat{\varepsilon}^{j+1}(n)$ with $\varepsilon^{j}(n)$ it suffices to restrict ourselves to adversaries that participate in one left and $m^{j+1}(n)$ right interactions (like the adversary A' above). Therefore,

$$\hat{\varepsilon}^{j+1}(n) \leq c \cdot m^{j+1}(n) \cdot \varepsilon^{j}(n) \ , \tag{27}$$

for some constant $c = O(1)$ dictated by proof of Theorem 13. More importantly, we note that $\hat{\varepsilon}^{j+1}(n)$ blows up by only a factor of $m^{j+1}(n) = \mathsf{id}^{j+1}(n)$ over $\varepsilon^{j}(n)$.

Combining Equations 27 and 26, we get

$$\varepsilon^{j+1}(n) \leq c \cdot \left(m^{j+1}(n)\right)^2 \cdot \varepsilon^{j}(n) \leq c \cdot \left(\mathsf{id}^{j+1}(n)\right)^2 \cdot \varepsilon^{j}(n) \ ,$$

Therefore,

$$\varepsilon^{j+1}(n) \leq c^{j} \cdot \prod_{0 \leq k \leq j+1} \left(\mathsf{id}^{k}(n)\right)^2 \cdot \varepsilon^{0}(n)$$

Plugging in $j+1 = r(n)$, we get

$$\varepsilon^{r(n)}(n) \leq c^{r(n)} \cdot \prod_{0 \leq k \leq r(n)} \left(\mathsf{id}^{k}(n)\right)^2 \cdot \varepsilon^{0}(n)$$

Since, $r(n) = O(\log^* n)$, $c = O(1)$ and $\varepsilon^0(n)$ are negligible functions we conclude that $\varepsilon^{r(n)}(n)$ is negligible. This then establishes the security of $\langle \widehat{C}^*, \widehat{R}^*\rangle$. This now concludes the proof of Theorem 17.

9 Two-round Robust CCA-secure Commitment

In this section we consider a stronger notion of security for commitments – security against adaptive chosen commitment attacks (CCA-security). CCA-security for commitment schemes was defined in [CLP10, LP12] and is analogous to the extensively studied notion of security under chosen-ciphertext attacks for encryption schemes. Roughly speaking, a tag based commitment scheme is CCA-secure if the value committed using an tag id remains hidden even if the receiver has access to an oracle that "breaks" any commitment using any tag $\mathsf{id}' \neq \mathsf{id}$, and returns the (unique)

value committed inside the commitment. We call such an oracle the *committed-value oracle*. CCA-security can be viewed as a natural strengthening of concurrent non-malleability – roughly speaking, a commitment scheme is concurrently non-malleable if it is CCA-secure with respect to restricted classes of adversaries that only make a single parallel (non-adaptive) query to the oracle after completing all interactions with the honest committer.

In this section, we show that the 2-round concurrent non-malleable commitment scheme described in Section 8 is in fact also CCA-secure. Recall that the 2-round scheme is constructed by iteratively applying the amplification transformation in Section 6 to the basic schemes for short identities in Section 5. The basic schemes for short identities are only one-one non-malleable which is amplified to concurrent non-malleability for n-bit identities by a two-step amplification procedure: first by applying the 2-round strengthening technique in Section 6.3 which strengthens the one-one non-malleability to concurrent non-malleability while preserving the length of identities; then applying the DDN *log n* trick (Section 7) to increase the length of identities while loosing concurrent non-malleability. The above two-step amplification step is iteratively applied for $O(\log^* n)$ times resulting in a scheme for n-bit identities but is only one-one non-malleable. To restore concurrent non-malleability the 2-round strengthening technique is applied once more. Since the strengthening technique is the final step in the construction, to show that the resulting scheme $\langle C^*, R^* \rangle$ is also CCA-secure, it is sufficient to show that the strengthening technique described in Section 6.3 produces a CCA-secure commitment scheme.

Below we first formally define the notion of CCA-secure commitments and then prove that the strengthening technique of Section 6.3 produces a CCA-secure scheme.

9.1 CCA-secure Commitment w.r.t. Committed-Value Oracle

Committed-value Oracle. Let $\langle C, R \rangle$ be a tag-based perfectly binding commitment scheme with $t(n)$-bit identities. Consider a non-uniform circuit family $A = \{A_n\}_{n \in \mathbb{N}}$. A committed-value oracle $\mathcal{O}$ of $\langle C, R \rangle$ acts as follows in interaction with A: For security parameter n, it participates with A in m-interactions acting as a honest receiver, using identities of length $t(n)$ which are adaptively chosen by A. At the end of each interaction, $\mathcal{O}$ returns the unique value committed in the interaction if it exists, otherwise it returns $\perp$. More precisely, $\mathcal{O}$ at the end of an interaction say with transcript c, computes the function val on c and returns $\mathsf{val}(c)$ to A. Recall that $\mathsf{val}(c)$ equals the (unique) value committed in c when c is a valid commitment, else $\mathsf{val}(c)$ is $\perp$.

A tag-based commitment scheme $\langle C, R \rangle$ is CCA-secure w.r.t. committed-value oracle, if the hiding property of the commitment scheme holds even with respect to adversaries that have access to the committed-value oracle $\mathcal{O}$. More precisely, let $A^{\mathcal{O}}$ denote the adversary A having access to the committed-value oracle $\mathcal{O}$. Consider the following probabilistic experiment $\mathsf{IND}(1^n, b)$, where $b \in \{0, 1\}$: For security parameter n, $A^{\mathcal{O}}$ adaptively[32] chooses a pair of challenge values $(v_0, v_1) \in \{0,1\}^\alpha$ – the values to be committed to – and an identity id of length $t(n)$, and interacts with the honest committer C to receive a commitment to v_b using identity id. Finally, the experiment outputs the output y of $A^{\mathcal{O}}$ where y is replaced with $\perp$ if A queries the oracle $\mathcal{O}$ on a commitment using an identity which is same as the identity id of the commitment it receives. We will denote the output of the above experiment by $\mathsf{IND}^A_{\langle C,R \rangle}(1^n, b)$.

Definition 21 (CCA-secure Commitments [LP12])**.** *Let $\langle C, R \rangle$ be a tag-based commitment scheme for $t(n)$-bit identities, and $\mathcal{C}$ a class of circuits. We say that $\langle C, R \rangle$ is $\mathcal{C}$-CCA-secure w.r.t. the committed-value oracle, if for every circuit family $A = \{A_n\}_{n \in \mathbb{N}} \in \mathcal{C}$ participating in $m = \mathsf{poly}(n)$*

[32] the choice of values v_0, v_1 and the identity id can depend on the right interactions of A with the committed value oracle.

interactions with the oracle while sending/receiving commitments to $\alpha = \mathsf{poly}(n)$-bit values, the following ensembles are computationally indistinguishable:

$$\left\{\mathsf{IND}^{A}_{\langle C,R\rangle}(1^n,0)\right\}_{n\in\mathbb{N}} \;;\; \left\{\mathsf{IND}^{A}_{\langle C,R\rangle}(1^n,1)\right\}_{n\in\mathbb{N}} . \tag{28}$$

As stated before and observed in [CLP10, LP12], CCA-security can be viewed as a natural strengthening of concurrent non-malleability. The proof is standard and is omitted but for completeness we state the theorem below.

Theorem 18. *Let $\langle C, R\rangle$ be a commitment scheme and $\mathcal{C}$ be a class of circuits that is closed under composition with $\mathcal{P}$/poly. Then if $\langle C, R\rangle$ is $\mathcal{C}$-CCA-secure w.r.t. the committed-value oracle then it is $\mathcal{C}$-concurrent non-malleable w.r.t. commitment.*

9.2 k-Robustness w.r.t. Committed-value Oracle

In the literature, CCA-security is usually used together with another property – *robustness* which captures security against a man-in-the-middle adversary that participates in an *arbitrary* left interaction with a *limited number of rounds*, while having access to the committed-value oracle. Roughly speaking, $\langle C, R\rangle$ is k-robust if the joint outputs of every k-round interaction, with an adversary having access to $\mathcal{O}$, can be simulated without the oracle. In other words, having access to the oracle does not help the adversary in participating in any k-round protocol much.

Definition 22 (Robustness)**.** *Let $\langle C, R\rangle$ be a tag based commitment scheme with $t(n)$-bit identities, and $\mathcal{C}$ and $\mathcal{C}'$ two classes of circuits. We say that $\langle C, R\rangle$ is $(\mathcal{C}, \mathcal{C}', k)$-robust w.r.t. the committed-value oracle, if there exists a simulator $S \in \mathcal{C}'$, such that, for every adversary $A \in \mathcal{C}$ that participates with $\mathcal{O}$ in $m = \mathsf{poly}(n)$ interactions and for every $B \in \mathcal{C}$ that participates in a k-round interaction with A the following ensembles are computationally indistinguishable,*

$$\left\{\mathsf{output}_{B,A^{\mathcal{O}}}[B, A^{\mathcal{O}}(1^n)]\right\}_{n\in\mathbb{N}} \;;\; \left\{\mathsf{output}_{B,S^{A}}[B, S^{A^{\mathcal{O}_S}}(1^n)]\right\}_{n\in\mathbb{N}} , \tag{29}$$

where $\mathsf{output}_{B,A^{\mathcal{O}}}[B, A^{\mathcal{O}}(1^n)]$ denote the joint outputs of A and B in an interaction between them with uniformly and independently chosen random inputs to each machine and $\mathcal{O}_S$ is the oracle simulated by S for A.

Remark 10. *In the standard definition of robustness [LP12], the probabilistic poly-time adversaries A and B are given auxiliary inputs – private inputs y and z respectively and common input x. Since, our adversaries our non-uniform we can assume that the values x, y, z are instead hardcoded in A and B.*

9.3 Proof of Robust CCA-security of $\langle \widehat{C}, \widehat{R}\rangle$

The commitment scheme $\langle \widehat{C}, \widehat{R}\rangle$ is a result of applying the strengthening technique described in Section 6.3 to a 2-round over-extractable $\mathcal{C}^{\wedge}_{S_{\mathsf{NM}},S_{\mathsf{NM}}}$ one-one non-malleable (w.r.t. extraction) commitment scheme $\langle C, R\rangle$. The strengthening technique additionally relies on other basic building blocks described in Section 6.2. It was shown in Theorems 12,13,14 that $\langle \widehat{C}, \widehat{R}\rangle$ is over-extractable w.r.t. extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ and is $\mathcal{C}^{\wedge}_{d_4,d_4}$ concurrent non-malleable w.r.t. extraction and commitment. Next, we will show that $\langle \widehat{C}, \widehat{R}\rangle$ is also $\mathcal{C}^{\wedge}_{d_4,d_4}$-CCA-secure and $(\mathcal{C}^{\wedge}_{d_4,d_4}, \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}, \kappa)$-robust for any polynomial κ.

Theorem 19. *$\langle \widehat{C}, \widehat{R} \rangle$ is $\mathcal{C}^{\wedge}_{d_4,d_4}$-CCA-secure and is $(\mathcal{C}^{\wedge}_{d_4,d_4}, \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}, \kappa(n))$-robust w.r.t. committed-value oracle for any polynomial κ.*

The proof of Theorem 19 consists of two parts: in Section 9.3.1 we first show that $\langle \widehat{C}, \widehat{R} \rangle$ is CCA-secure and in Section 9.3.2 we show that it is also robust.

9.3.1 Proof of CCA-security

Let us consider a fixed family of circuits $A = \{A_n\}_{n\in\mathbb{N}}$ belonging to the circuit class $\mathcal{C}^{\wedge}_{d_4,d_4}$ that in the CCA-experiment $\mathsf{IND}(1^n, b)$ interacts with a honest receiver C and has oracle access to the committed-value oracle to which it makes $m = \mathsf{poly}(n)$ number of queries. For convenience, we will refer to A's interaction with C as the *left* interaction and its interactions with $\mathcal{O}$ as *right* interactions. Then, to prove CCA-security, we need to show that

$$\{\mathsf{IND}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 0)\}_{n\in\mathbb{N}} \approx_c \{\mathsf{IND}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 1)\}_{n\in\mathbb{N}} \ . \tag{30}$$

Proof Overview. At a very high level: the above indistinguishability follows from similar proof as that of one-many non-malleability in Section 6.3. The proof goes through similar hybrids $\{H_j\}_j$ as that for proving non-malleabilty in the proof of Theorems 13 and 14, with the following slight modification. In the definition of non-malleability, the man-in-the-middle A interacts with the honest receivers on the right, whereas in that for CCA security, A interacts with the committed-value oracle $\mathcal{O}$ on the right, who additionally returns the value val committed in every right interaction as soon as it ends. Therefore, in the hybrids for proving CCA-security, we need to simulate $\mathcal{O}$ for A. To do so, we rely on the over-extractability of $\langle \widehat{C}, \widehat{R} \rangle$ by an extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$, and simulate the committed-value oracle for A using the following *extracted-value oracle* — $\mathcal{O}_E$ works identically to the committed-value oracle except that at the end of an interaction, it runs $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ to extract a value from the commitment and returns it to A.

With the modified hybrids, to show CCA-security, we need to establish that i) $\mathcal{O}_E$ indeed simulates the committed-value oracle correctly, and ii) the indistinguishability of the hybrids remains. For i), recall that the over-extractability of $\langle \widehat{C}, \widehat{R} \rangle$ only guarantees that the value $\mathcal{O}_E$ extracts is the correct committed value when a commitment is valid, otherwise, $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ might return an arbitrary value, instead of $\perp$. To show that the latter does not happen, (similar to the proof of non-malleability in Theorem 13 and 14,) we maintain throughout all hybrids a "no-fake-witness" invariant, which would guarantee that $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ indeed returns $\perp$ when a right commitment is invalid, except with negligible probability. Hence, $\mathcal{O}_E$ perfectly simulates the committed-value oracle with overwhelming probability.

Next, to show ii) the indistinguishability of the hybrids, recall that the extractor $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ on a commitment c works as follows: It returns $\perp$ if the ZAP proof (in c) is not accepting, and otherwise, it return the value v' extracted from $c1$ using the extractor $o\mathcal{E}_1$ of ECom_1 — the complexity of $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ is roughly the same as that of $o\mathcal{E}_1$. Observe that running the extractor $o\mathcal{E}_1$ of ECom_1, and hence $\widehat{o\mathcal{E}}_{\mathsf{NM}}$, in the hybrids does not hurt the security of any other components, namely, $\mathsf{CRH}, \langle C, R\rangle$ and ECom_i's for $i > 1$, since $\mathsf{ECom}_1 \prec \mathsf{CRH}, \langle C, R\rangle, \mathsf{ECom}_2, \mathsf{ECom}_4, \mathsf{ECom}_3$, as depicted in Figure 2 (iii). Therefore, if the indistinguishability of a pair of neighboring hybrids reduces to the security of components other than ECom_1, this indistinguishability remains intact even when running $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ inside. This is the case for all but the last two hybrids, whose indistinguishability reduces to the hiding of ECom_1 itself. To show their indistinguishability, (again similar to the proof of non-malleability,) we simulate $\widehat{o\mathcal{E}}_{\mathsf{NM}}$ by extracting from the commitment $c3$ using the extractor $o\mathcal{E}_3$ for

ECom_3, and rely on the hiding of ECom_1 against $o\mathcal{E}_3$. This concludes the overview of the proof of CCA-security. Next, we provide a more formal analysis.

Proof Sketch We consider a sequence of hybrids $\{G_j(b)\}_{0\leq j\leq 6}$ for $b \in \{0,1\}$ where for every $0 \leq j \leq 6$ and $b \in \{0,1\}$ the hybrid $G_j(b)$ is identical to the hybrid $H_j(b)$ described in the Proof of Theorem 13 in Section 6.3 except one slight difference. For its right interactions A in $G_j(b)$ interacts with the extracted-value oracle $\mathcal{O}_E$ instead of the honest receiver as in $H_j(b)$. Note that the hybrid $G_0(b)$ as described above emulates an execution which is identical to the CCA-experiment $\mathsf{IND}(b)$[33] with A except A is given access to the extracted-value oracle $\mathcal{O}_E$ instead of the committed-value oracle. As before, for notational convenience, we use font style x to denote a random variable in the left interaction, and font style $\tilde{x}_i$ the corresponding random variable in the i'th right interaction. Moreover, by $\mathsf{IND}^A_{G_j}(1^n, b)$ we will denote the output of the hybrid $G_j(b)$. Then to show indistinguishability as described in Equation (30), we prove in Lemma 5 that the output of the neighbouring hybrids $G_j(b)$ and $G_{j+1}(b)$ are indistinguishable for the same b. Furthermore, we show the output is statistically close in $G_6(1)$ and $G_5(0)$ and the output of $G_0(b)$ is also statistically close to $\mathsf{IND}^A_{\langle\widehat{C},\widehat{R}\rangle}(b)$, this then establishes Equation (30).

Lemma 5. *For $b \in \{0,1\}$ and $0 \leq j \leq 5$, the following are computationally indistinguishable,*

$$\mathsf{IND}^A_{G_j}(b)\ ;\ \mathsf{IND}^A_{G_{j+1}}(b)\ ,$$

and $\mathsf{IND}^A_{G_0}(b) \approx_s \mathsf{IND}^A_{\langle\widehat{C},\widehat{R}\rangle}(b)$ and $\mathsf{IND}^A_{G_6}(b) \approx_s \mathsf{IND}^A_{G_5}(0)$.

Towards proving the above lemma, we will also maintain the following "no-fake-witness" invariant (similar to Invariant 1 in Section 6.3).

Invariant 3 (No-fake-witness invariant)**.** *In $G_j(b)$, the probability that there exists a right interaction i that is accepting and A commits to a fake witness in it is negligible.*

Showing the no-fake-witness invariant in every hybrid enforces A to prove the honest statement in every accepting right interaction k. That is, for every accepting right interaction k, A proves that the underlying commitment $\widetilde{c1}_k$ is valid. Then, due to the over-extraction property of the extractor $o\mathcal{E}_1$, it follows that A in its interaction with the extracted-value oracle in fact receives the value actually committed inside the right commitment $\tilde{c}_k$. Therefore A's interaction with the extracted-value oracle is identical to its interaction with the committed-value oracle, except with negligible probability. This fact will come in handy to show Lemma 5.

In fact, as in the proof of Theorems 13 and 14, we maintain the following, easier to prove, invariant which from an argument similar to the one made in the proof of Claim 2, implies Invariant 3.

Invariant 4. *In $G_j(b)$, the probability that there exists a right interaction i that is accepting and the value* extracted *from the non-malleable commitment $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ in this interaction is a fake witness is negligible.*

Therefore to establish the proof of CCA-security, we will prove Lemma 5 and show that Invariant 4 holds in all hybrids.

First, we show that Invariant 4 holds in $G_0(b)$. In fact, as in Claim 3, we show that the value extracted from the ECom_2 commitment $\widetilde{c2}_k$ in any right interaction k is not a collision of the hash function $\widetilde{h}_k$ where A interacts with $\mathcal{O}_E$ for its right interactions. This then implies Invariant 4

[33] We ignore the security parameter for notational convenience

holds. At a high level this readily follows from the fact that the collision-resistance of the hash function is more secure than both ECom_2 and ECom_1, $h \succ \mathsf{ECom}_2, \mathsf{ECom}_1$ (see Figure 2 (iii)). This is because if in some right interaction k, A commits to a collision of $\widetilde{h}_k$ using ECom_2, then we can construct a non-uniform circuit B' that violates the collision-resistance of $\widetilde{h}_k$ by extracting from $\widetilde{c2}_k$. More precisely, B' behaves identically to the adversary B in the proof of Claim 3 except that for all its $m = \mathsf{poly}(n)$ right interactions with A, B' internally simulates the oracle $\mathcal{O}_E$ by running the extractor $o\mathcal{E}_1$ whereas B just acts as a honest receiver. Therefore, the size of B' blows up by an additive factor of $m \cdot \mathsf{size}(o\mathcal{E}_1)$ over the size of B. Since size of B is at most $\mathsf{poly}(S_{\mathsf{CRH}})$ and the size of $o\mathcal{E}_1$ is also at most $\mathsf{poly}(S_{\mathsf{CRH}})$, we have that B' also has size $\mathsf{poly}(S_{\mathsf{CRH}})$, that is,

$$\begin{aligned}
\mathsf{size}(B') &\leq \mathsf{size}(B) + m \cdot \mathsf{size}(o\mathcal{E}_1) \\
&\leq \mathsf{size}(A) + \mathsf{size}(o\mathcal{E}_2) + \mathsf{poly}(n) + m \cdot \mathsf{size}(o\mathcal{E}_1) \\
&\leq \mathsf{poly}(d_4) + \mathsf{poly}(S_1) + \mathsf{poly}(S_{\mathsf{CRH}}) \\
&< \mathsf{poly}(S_{\mathsf{CRH}}) \qquad (\text{since, } S_{\mathsf{CRH}} >> S_1, d_4 \text{ from Equation (9)}).
\end{aligned}$$

Therefore, $B \in \mathcal{C}^{\wedge}_{S_{\mathsf{CRH}}, S_{\mathsf{CRH}}}$ and then due to the $\mathcal{C}_{S_{\mathsf{CRH}}}$-collision-resistance of $\mathcal{H}$ we have that Invariant 4 holds in $G_0(b)$ as formalized in the following claim,

Claim 17. *For $b \in \{0,1\}$ and for every right interaction i in $G_0(b)$, the probability that i is accepting and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

We recall that the only difference between showing Invariant 4 holds in $G_0(b)$ from the proof of Claim 3 was that the adversary B' (defined similarly to adversary B from Claim 3) additionally runs the extractor $o\mathcal{E}_1$ to simulate the extracted value oracle for A for its right interactions. In fact one can show Invariant 4 holds in hybrids $G_1(b)$ through $G_5(b)$ via the same modification to adversary constructed in the proof of Claims 4, 6, 8, 10 and 12 respectively. Since, $\mathsf{ECom}_1 \prec \langle C, R\rangle, \mathsf{ZAP}, \mathsf{ECom}_i$ $(i > 1)$, it can be observed that running the extractor $o\mathcal{E}_1$ of $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ does not blow up the size or depth of the modified adversary much still allowing us to reach a contradiction as in the above Claims from Section 6.3. Furthermore, $G_6(b)$ is in fact identical to $G_5(0)$ (as $H_5(0)$ identical to $H_6(b)$), therefore Invariant 4 also holds in $G_6(b)$. Therefore essentially by the same proofs in Section 6.3, we conclude that Invariant 4 does hold in all hybrids $G_j(b)$. This is captured in the following Claim and we skip a formal proof.

Claim 18. *For $b \in \{0,1\}, 0 \leq j \leq 6$ and for every right interaction i in $G_j(b)$, the probability that i is accepting and the value extracted from $(\widetilde{a}_{\mathsf{NM}i}, \widetilde{b}_{\mathsf{NM}i})$ is a fake witness, is negligible.*

Next we move onto showing Lemma 5. First, given Claim 17 holds, we show that the output of hybrid $G_0(b)$ is statistically close to the CCA-experiment $\mathsf{IND}(b)$ for any $b \in \{0,1\}$.

Claim 19. *For $b \in \{0,1\}$, the following holds*

$$\mathsf{IND}^A_{G_0}(b) \approx_s \mathsf{IND}^A_{\langle \widehat{C}, \widehat{R}\rangle}(b) \ .$$

Note that due to Claim 17 and also because Invariant 4 implies Invariant 3, we know that A in each of its (accepting) right interactions, with the oracle $\mathcal{O}_E$, does not commit to a fake witness, except with negligible probability. Then by the soundness of ZAP, in every accepting right interaction k, A proves with overwhelming probability that the underlying commitment $\widetilde{c1}_k$ is well-formed . Therefore by the over-extractability of ECom_1 w.r.t. $o\mathcal{E}_1$, we know that the extracted

value oracle $\mathcal{O}_E$ (implemented using $o\mathcal{E}_1$) in fact returns $\mathsf{val}(\widetilde{c1}_k) = \mathsf{val}(\widetilde{c}_k)$. For interactions k that are not accepting, both val and $\mathcal{O}_E$ return $\perp$. Therefore for every right interaction k, the values returned by the extracted-value oracle $\mathcal{O}_E$ agree with $\mathsf{val}(c_k)$, the values returned by the committed-value oracle $\mathcal{O}$ except with negligible probability. Therefore, interaction of A with the extracted-value oracle $\mathcal{O}_E$ is statistically close to its interaction with the committed-value oracle $\mathcal{O}$ implying Claim 19.

Next we show that the output of $G_0(b)$ is indistinguishable from the output of $G_1(b)$, that is, $\mathsf{IND}^A_{G_0}(b)$ and $\mathsf{IND}^A_{G_1}(b)$ are indistinguishable. As in Claim 5, we construct an adversary B' that violates the hiding of ECom_2, that is, B' works identically to the adversary B in the proof of Claim 5 except Step 4 and 5. The adversary B (in Claim 5) waits for A to terminate and then in its Step 4 runs $o\mathcal{E}_1$ to obtain $\tilde{v_i}'$ for every successful right interaction i and sets $\tilde{v_i}' = \perp$ for every unsuccessful right interaction i. Then in Step 5, B runs the distinguisher D on the view of A and right extracted values $\tilde{v_i}'$ and returns the output of D. However, here in the CCA case, A expects to receive the extracted values and that too as soon as a right interaction ends. Therefore, B' runs the extractor $o\mathcal{E}_1$ to obtain $\tilde{v_i}'$ as soon as the i-th interaction ends and returns $\tilde{v_i}'$ to A if i is an accepting right interaction. Otherwise, it returns $\perp$. Then it runs the distinguisher D on the output y of A which is carefully replaced with $\perp$ if any of A's right interactions uses the same identity as its left interaction. The former change of running the extractor $o\mathcal{E}_1$ to obtain $\tilde{v_i}'$ is similar to the modification made while proving that Invariant 4 holds in $G_j(b)$ (Claim 18) and the later change is merely a syntactic change required to be consistent with the IND experiment. Note that this change in the code of B' does not blow up its depth significantly (over B). Since depth of B is at most $\mathsf{poly}(d_2)$ and $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$, we have that $\mathsf{dep}(B')$ is at most $\mathsf{poly}(d_2)$. Then the $\mathcal{C}^{\vee}_{d_2,S_2}$-hiding of ECom_2 implies that the output of $G_0(b)$ and $G_1(b)$ are indistinguishable as formalized in the following claim,

Claim 20. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{IND}^A_{G_0}(b); \mathsf{IND}^A_{G_1}(b) \ .$$

We recall that the only difference in showing indistinguishability of $\mathsf{IND}_{G_0}(b)$ and $\mathsf{IND}_{G_1}(b)$ from the proof of Claim 5 was that the adversary B' (defined similarly to adversary B from Claim 5) additionally runs the extractor $o\mathcal{E}_1$ to simulate the extracted value oracle for A for its right interactions and runs the distinguisher D on the output of A instead of running D on the view of A and the values extracted from its right interactions. In fact one can show that $\mathsf{IND}_{G_1}(b)$ through $\mathsf{IND}_{G_5}(b)$ are all indistinguishable via the same modification to adversary constructed in the proof of Claims 7, 9, 11, 13 respectively. Since, $\mathsf{ECom}_1 \prec \langle C, R\rangle, \mathsf{ZAP}, \mathsf{ECom}_i$ $(i > 1)$, it can be observed that running the extractor $o\mathcal{E}_1$ of $(\mathsf{ECom}_1, \mathsf{EOpen}_1)$ does not blow up the size or depth of the modified adversary much still allowing us to reach a contradiction as in the above Claims from Section 6.3.

Claim 21. *For $j \in [4], b \in \{0,1\}$ the following holds*

$$\mathsf{IND}^A_{G_i}(b) \approx_c \mathsf{IND}^A_{G_{i+1}}(b) \ .$$

One would like to extend the above arugment to even argue the indistinguishability of $\mathsf{IND}_{G_5}(b)$ and $\mathsf{IND}_{G_6}(b)$ based on the proof of Claim 15 which reduces to the hiding of ECom_1. However, running $o\mathcal{E}_1 \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ on the right blow up the size and depth of B' significantly, that is, $\mathsf{size}(B') \geq$

$\mathsf{size}(o\mathcal{E}_1) = \mathsf{poly}(S_{\mathsf{CRH}}) >> S_1$ and similarly $\mathsf{dep}(B') >> d_1$. Since $B' \notin \mathcal{C}^{\vee}_{d_1,S_1}$, it does not violate the $\mathcal{C}^{\vee}_{d_1,S_1}$-hiding of ECom_1. To fix this issue we consider two intermediate hybrids $G'_5(b)$ and $G'_6(b)$ which are statistically close to $G_5(b)$ and $G_6(b)$ respectively and then argue how proof of Claim 15 can be extended to argue the indistinguishability of $\mathsf{IND}_{G_5}(b)$ and $\mathsf{IND}_{G_6}(b)$.

Hybrid $G'_j(b)$ for $5 \leq j \leq 6$: The hybrids $G'_j(b)$ are identical to $G_j(b)$ for $5 \leq j \leq 6$ except the implementation of the extracted-value oracle. Here, the extracted-value oracle behaves as before except that for an accepting right interaction i, the extractor $o\mathcal{E}_3$ is run on the underlying $\widetilde{c3}_i$ commitment to extract the value $(\tilde{v_i}', \widetilde{d1_i}')$ and the value $\tilde{v_i}'$ is returned.

Given that Invariant 4 holds in $G_j(b)$ (Claim 18), A in each of its (accepting) interaction with the oracle $\mathcal{O}_E$ does not commit to the fake witness, except with negligible probability. Therefore, by the soundness of ZAP, in every accepting right interaction k, A proves that the underlying commitments $\widetilde{c1}_k$ and $\widetilde{c3}_k$ are well-formed and $\widetilde{c3}_k$ commits to a decommitment of $\widetilde{c1}_k$. Then due to the over-extractability of ECom_3 w.r.t. $o\mathcal{E}_3$ we know that the value $(\tilde{v_k}', \widetilde{d1_k}')$ extracted by $o\mathcal{E}_3$ is in fact the decommitment of $\widetilde{c1}_k$ which implies that $\tilde{v_k}'$ is in fact the value committed inside $\tilde{c1}_k$. Since the commitment $\tilde{c1}_k$ is also well-formed (as described above), the over-extractability of ECom_1 w.r.t. $o\mathcal{E}_1$ implies that the value extracted from $\tilde{c1}_k$ is also equal to $\mathsf{val}\tilde{c1}_k$ except with negligible probabilty. Therefore, the value $\tilde{v_k}'$ (extracted by $o\mathcal{E}_3$) is equal to the value extracted by $o\mathcal{E}_1$ in every right interaction which implies that the view of A in hybrids $G_j(b)$ and $G'_j(b)$ remains identical except with negligible probability. Therefore the following follow,

Claim 22. *For $b \in \{0,1\}$ and $5 \leq j \leq 6$, the following holds,*

$$\mathsf{IND}^A_{G_j}(b) \approx_s \mathsf{IND}^A_{G'_j}(b) \ .$$

Next we show that $\mathsf{IND}^A_{G'_5}(b)$ and $\mathsf{IND}^A_{G'_6}(b)$ are indistinguishable. This follows from the fact that ECom_1 is more secure than ECom_3, $\mathsf{ECom}_1 \succ \mathsf{ECom}_3$ (see Figure 2 (iii)). More precisely we construct an adversary B' that violates the hiding of ECom_1 where B' works identically to the adversary B in the proof of Claim 15 except a slight difference. Here, B' to simulate the extracted-value oracle runs the extractor $o\mathcal{E}_3$ to obtain $\tilde{v_i}'$ as soon as the i-th interaction ends unlike B which runs the extractor $o\mathcal{E}_3$ after all the right interactions end. This change in the code of B' does not blow up its size and depth significantly (over B) and therefore B' (like B) falls in the class $\mathcal{C}^{\vee}_{d_1,S_1}$. Then the $\mathcal{C}^{\vee}_{d_1,S_1}$-hiding of ECom_1 implies that the output of $G'_5(b)$ and $G'_6(b)$ are indistinguishable.

Claim 23. *For $b \in \{0,1\}$, the following are indistinguishable,*

$$\mathsf{IND}^A_{G'_5}(b); \mathsf{IND}^A_{G'_6}(b) \ .$$

Then combining Claims 19, 20,21,22 and 23 and observing that $\mathsf{IND}_{G_5}(0)$ is identical to $\mathsf{IND}_{G_6}(b)$ (as $G_5(0)$ is identical to $G_6(b)$ concludes the proof of Lemma 5 and hence the proof of CCA-security of $\langle \widehat{C}, \widehat{R} \rangle$.

9.3.2 Proof of Robustness

To show that $\langle \widehat{C}, \widehat{R} \rangle$ is $(\mathcal{C}^{\wedge}_{d_4,d_4}, \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}, \kappa(n))$-robust, we need to show that for every $k \leq \kappa(n)$ there exists a simulator $S \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ such that for any $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and for any $B \in \mathcal{C}^{\wedge}_{d_4,d_4}$ that participates in a k-round interaction, interaction between B and A where A has access to the committed value

oracle $\mathcal{O}$ is indistinguishable from that between B and S. In other words, S is able to simulate the committed value oracle $\mathcal{O}$ for A when its interacting with an arbitrary B. The construction of the simulator S is very similar to the hybrid $G_0(b)$ as described in the proof of CCA-security in Section 9.3.1. More precisely, given k and a circuit $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$, S externally interacts with an arbitrary k-round circuit B and internally simulates an execution between B and A by forwarding messages from B to A. For the right interactions, S internally simulates the extracted value oracle $\mathcal{O}_E$ for A as described in Section 9.3.1.

To conclude the proof of robustness we need to show two things: (1) $S \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ and (2) S indeed is able to simulate the committed-value oracle $\mathcal{O}$ for A. First, it is easy to see that S runs $A \in \mathcal{C}^{\wedge}_{d_4,d_4}$ and simulates the extracted-value oracle $\mathcal{O}_E$ for $\mathsf{poly}(m)$ right interactions. As $\mathcal{O}_E$ can be simulated by a circuit in $\mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$ we have that $S \in \mathcal{C}^{\wedge}_{d_2,S_{\mathsf{CRH}}}$. Second, by an argument simular to the one made in the Proof of Claim 17 one can show that due to collision resistance of $\mathcal{H}$ A does not commit to a fake witness in any of its right interactions. Then, as in Claim 19 we can conclude that the view of A with the committed-value oracle is statistically close to the view of A with the extracted-value oracle (as simulated by S). This then concludes the proof of robustness and the proof of Theorem 19.

On the robustness of the scheme $\langle C^*, R^* \rangle$. We claim that the final commitment scheme $\langle C^*, R^* \rangle$ is $(\mathcal{P}/\mathrm{poly}, \mathcal{C}', \kappa(n))$-robust w.r.t the committed-value oracle where $\mathcal{C}'$ is the set of all non-uniform circuits whose size is upperbounded by $\mathsf{poly}(2^{(\log n)^c})$ for a sufficiently large constant c. In other words, $\langle C^*, R^* \rangle$ is robust w.r.t. quasi-polynomial time simulation. Recall that the commitment $\langle C^*, R^* \rangle$ is constructed by repeatedly applying the transformations presented in Sections 6.3 and 7 relying on a $L = O(\log^* n)$ hierarchy $p_1 << \ldots << p_L$ of non-decreasing functions as discussed in Section 8.2 where each level $p_i = 2^{n_i^{\varepsilon}}$ for an appropriate security parameter n_i. Furthermore recall that the final step in the construction of $\langle C^*, R^* \rangle$ is applying the strengthening technique which relies on a hierarchy of functions as described in Equation (9). For this last step the corresponding functions $d_4, \ldots, d_2, \ldots, S_{\mathsf{CRH}}$ are instantiated from the first few functions in the hierarchy namely $p_1, \ldots, p_4, \ldots, p_7$. Setting n_is as discussed in Section 8.2 will ensure that d_2 and S_{CRH} are both than $\mathsf{poly}(2^{(\log n)^c})$[34] for some sufficiently large constant c. Hence, the simulator for $\langle C^*, R^* \rangle$ belongs to the class $\mathcal{C}'$ as described above.

10 Non-interactive Concurrent Non-Malleable and CCA-secure Commitment against Uniform Adversaries

In this section, we show that when restricting attention to uniform attackers, the first message in our 2-round concurrent non-malleable commitment scheme constructed in Section 8 can be removed (Theorem 2). Recall that these 2-round protocols are obtained by iteratively applying the amplification transformation in Section 6 to the basic schemes for short identities in Section 5. While the basic schemes are in fact non-interactive, the amplification technique, however, produces schemes with 2 rounds. Our amplification technique involves two steps: Applying the DDN $\log n$ trick, which is actually round preserving, and the security strengthening step that lifts one-one non-malleability w.r.t. extraction to concurrent non-malleability w.r.t. extraction and commitment, while preserving the length of identities. In the security strengthening step, the output scheme has two rounds, where the first message is sent by the receiver and contains the index of a randomly sampled function h from a family of non-uniform CRHFs, the first message of a ZAP proof, and

[34] Setting n_0 to, say, $(\log n)^2$ in Section 8.2.

the first message of the input non-malleable commitment scheme (if there is any). Therefore, to remove the first message, our idea is to simply replace h for a fixed uniform CRHF, and replace ZAP with a NIWI, so that the transformation when applied to a non-interactive input commitment scheme, produces a non-interactive output scheme. The only drawback is that with the use of uniform CRHF, the output scheme is only secure against uniform adversaries. We also show that the output scheme of the modified strengthening technique also satisfies stronger notions of CCA-security and robustness when adversaries are restricted to be uniform Turning machines.

Below, we first adapt the notions of non-malleability w.r.t. extraction and commitment, and robust CCA-security to the setting of uniform attackers, and then describe the new amplification step.

10.1 Non-malleability against Uniform Adversaries

The notion of non-malleability w.r.t. commitment (or w.r.t. extraction) against *uniform* attackers is defined identically to that against non-uniform attackers as in Definition 16 (or Definition 17 resp.) in Section 3.5. To make the distinction explict between uniform and non-uniform we let $\mathsf{uMIM}^{A}_{\langle C,R\rangle}(1^n, b)$ represent the MIM experiment with a uniform adversary A (hence uMIM). We further denote by $\mathsf{umim}^{A}_{\langle C,R\rangle}(1^n, b)$ (or $\mathsf{uemim}^{A}_{\langle C,R\rangle}(1^n, b)$ resp.) the random variable describing the view of A together with the values committed in (or extracted from resp.) the right interactions.

Definition 23 (Non-malleability)**.** *A tag-based commitment scheme $\langle C, R\rangle$ is said to be concurrent T-non-malleable against uniform attackers if for every $\mathsf{poly}(T)$-time uniform Turing machine A participating in $m = \mathsf{poly}(n)$ while sending/receiving commitments to $\alpha = \mathsf{poly}(n)$-bit values, concurrent interactions, the following ensembles are computationally indistinguishable:*

$$\left\{\mathsf{umim}^{A}_{\langle C,R\rangle}(1^n, 0)\right\}_{n\in\mathbb{N}} \;;\; \left\{\mathsf{umim}^{A}_{\langle C,R\rangle}(1^n, 1)\right\}_{n\in\mathbb{N}} .$$

Moreover, it is said to be concurrent T-non-malleable w.r.t. extraction against uniform attackers, if the above indistinguishability holds between $\mathsf{uemim}^{A}_{\langle C,R\rangle}(1^n, 0)$ and $\mathsf{uemim}^{A}_{\langle C,R\rangle}(1^n, 1)$.

10.2 Robust CCA-security against Uniform Adversaries

Next we define the notions of CCA-security and Robustness against uniform advesaries. The definition are identical to the non-uniform case as defined in Definitions 21 and 22 except that A in the CCA definition is a uniform Turing machine and all A, B and S in the robustness definition are uniform Turing machines. For completness we define them below.

Definition 24. *We say that $\langle C, R\rangle$ is T-CCA-secure w.r.t. the committed-value oracle against uniform attackers if Equation (28) holds for all $\mathsf{poly}(T)$-time uniform Turing machines A that participate in $m = \mathsf{poly}(n)$ queries to the oracle $\mathcal{O}$.*

Definition 25. *We say that $\langle C, R\rangle$ is (T, T', k)-robust w.r.t. the committed-value oracle against uniform attackers if there exists $\mathsf{poly}(T')$-time uniform Turing machine S such that Equation (29) holds for all $\mathsf{poly}(T)$-time uniform Turning machines A and B which participates in a k-round interaction.*

10.3 1-Message Security Strengthening Technique

We now present our one-message transformation for security strengthening. For some hierarchy of non-decreasing functions on $\mathbb{N}$ satisfying,

$$\begin{aligned} &n << d_4 << d_3 << d_1 << d_2 << S_2 << S_1 << S_{\mathsf{CRH}} << \\ &S'_{\mathsf{CRH}} << S_{\mathsf{NM}} << S'_{\mathsf{NM}} << S_3 << S_4 << S'_4 << S^* \ , \end{aligned} \tag{31}$$

the transformation relies on the following building blocks:

1. $(\mathsf{oNICom}, \mathsf{oNIOpen})$ is a non-interactive, tag-based commitment scheme for $t(n)$-bit identities that is S'_{NM}-over-extractable by extractor $o\mathcal{E}_{\mathsf{NI}}$. Furthermore, $\langle C, R \rangle$ is one-one S_{NM}-non-malleable w.r.t. extraction by $o\mathcal{E}_{\mathsf{NI}}$ against uniform adversaries.
2. $\{(\mathsf{ECom}_i, \mathsf{EOpen}_i)\}_{1 \leq i \leq 4}$ are identical to that in Section 6.3.
3. NIWI is a non-interactive $\mathcal{C}_{S^*}$-witness-indistinguishable proof.
4. $\mathcal{H} = \{h_n\}_n$ is a S_{CRH}-uniform-collision resistant hash function such that there exists a $\mathsf{poly}(S'_{\mathsf{CRH}})$-time TM which finds collisions for $\mathcal{H}$ with probability 1.

Using the above mentioned building blocks, the transformation produces the scheme $(\mathsf{cNICom}, \mathsf{cNIOpen})$ which is non-interactive, tag-based commitment scheme for $t(n)$-bit identities that is S_{CRH}-over-extractable w.r.t. an extractor $\widehat{o\mathcal{E}}_{\mathsf{NI}}$. Furthermore, $(\mathsf{cNICom}, \mathsf{cNIOpen})$ is concurrent d_4-non-malleable w.r.t. extraction by $\widehat{o\mathcal{E}}_{\mathsf{NI}}$ and concurrent d_4-non-malleable (w.r.t. commitment) against uniform attackers.

The committer $\widehat{C}$ and the receiver $\widehat{R}$ receive the security parameter 1^n and identity $\mathsf{id} \in \{0,1\}^{t(n)}$ as common input. Furthermore, $\widehat{C}$ gets a private input $v \in \{0,1\}^n$ which is the value to be committed.

- Commit stage:

  1. $\widehat{C}$ computes a commitment $c1$ to the value v using ECom_1. Let $d1$ be the corresponding decommitment string.
  2. $\widehat{C}$ computes a commitment $c3$ to the decommitment $(v, d1)$ of $c1$ using ECom_3.
  3. $\widehat{C}$ computes a commitment $c2$ to a random string $r1$ using ECom_2.
  4. $\widehat{C}$ computes a commitment $c\mathsf{NM}$ to a random string $r3$ using oNICom using identity id.
  5. $\widehat{C}$ computes a commitment $c4$ to a random string $r3$ using ECom_4.
  6. $\widehat{C}$ computes the NIWI proof π to prove the following OR-statement:
     (a) *either* there exists a string $\bar{v}$ such that $c1$ is a commitment to $\bar{v}$ and $c3$ commits to a decommitment of $c1$.
     (b) *or* there exists a string $\bar{s} = (x_1, x_2)$ such that $c2$ is a commitment to $\bar{s}$, $c4$ commits to a decommitment of $c2$, $c\mathsf{NM}$ commits to a decommitment of $c4$ and $H_n(x_1) = H_n(x_2)$.

     $\widehat{C}$ proves the statement (a) by using a decommitment of $c3$ to $(v, d1)$ — decommitment of $c1$ to v — as the witness.
  7. $\widehat{C}$ sends $(c1, c2, c3, c4, c\mathsf{NM}, \pi)$ as commitment to $\widehat{R}$ and keeps the decommitment $(v, d1)$ private.

- Reveal stage:
  On receiving $(v, d1)$ from $\widehat{C}$, $\widehat{R}$ accepts the decommitment if the NIWI proof is accepting and if $\mathsf{EOpen}_1(c1, v, d1) = 1$. Otherwise, it rejects.

- Extraction - Extractor $\widehat{o\mathcal{E}_{\mathsf{NI}}}$:
  On receiving a commitment c and identity id, $\widehat{o\mathcal{E}_{\mathsf{NI}}}$ first verifies the NIWI proof and outputs $\perp$ if the proof is not accepting. Otherwise, it runs the extractor $o\mathcal{E}_1$ on $c1$ and outputs the extracted value v'.

Theorem 20. *$\langle \widehat{C}, \widehat{R} \rangle$ is a non-interactive, (d_2, S_{CRH})-over-extractable, perfectly binding commitment scheme for identities of length $t(n)$. Furthermore, it is concurrent d_4-non-malleable (w.r.t. commitment) and non-malleable w.r.t. extraction by extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$ against uniform adversaries.*

It is easy to see that $\langle \widehat{C}, \widehat{R} \rangle$ is perfectly binding and (d_2, S_{CRH})-over-extractable. The non-malleability properties follow syntactically from the same proof as that of Theorem 13 and 14 w.r.t. the 2-round security strengthening technique in Section 6.3. The only slight difference is that when reducing to the collision resistance of the hash function, and the non-malleability w.r.t. extraction of the input commitment scheme, we need to ensure that the reduction is a uniform Turing machine, which can be done easily. More specifically, in Section 6.3,

- we rely on the collision resistance of hash functions in order to show that Invariant 2 holds in hybrid $H_0(b)$ (Claim 3), and

- we rely on the non-malleability w.r.t. extraction of the input commitment scheme in order to show that Invariant 2 holds in $H_3(b)$ (Claim 8) and that the emim random variable is indistinguishable in $H_2(b)$ and $H_3(b)$ (Claim 9).

We now observe that the reductions presented in the proof of Claim 3, 8 and 9 can be made uniform. First, these reductions run internally 1) the adversary, 2) the extractors for different commitment schemes, 3) possibly a strategy for finding collisions (for the second bullet point), and some other computations, all of which can be implemented using uniform Turing machines. Furthermore, these reductions have one value hardwired in — the index k of a "special" right interaction. When adapting to the uniform setting, since there are only $m = \mathsf{poly}(n)$ number of right interactions, instead of hard-wiring k, the reduction can simply guess k at random, at the cost of losing a factor of m in its advantage. Therefore, by essentially the same proof, we can show the same in the uniform setting. We hence omit the complete proof.

Robust CCA-security. We next show that the commitment scheme $\langle \widehat{C}, \widehat{R} \rangle$ is also robust-CCA secure against uniform adversaries.

Theorem 21. *$\langle \widehat{C}, \widehat{R} \rangle$ is d_4-CCA-secure and $(d_4, S_{\mathsf{CRH}}, \kappa(n))$-robust w.r.t. committed value oracle against uniform adversaries.*

The proof of d_4-CCA security is identical to the proof of the CCA-security w.r.t. the 2-round strengthening technique as described in Section 9.3.1, except a slight difference. The difference is identical as in the above proof of non-malleability against uniform adversaries, that is, to deal with the uniform collision resistance of hash function and uniform one-one non-malleability w.r.t. extraction of the input commitment scheme As observed earlier, we need to ensure that the reductions are uniform Turning machines which can be easily done as described above. The proof

of $(d_4, S_{\mathsf{CRH}}, \kappa(n))$-robustness also follows from the proof of robustness described in Section 9.3.2 except that the simulator S also needs to be a uniform Turing machine which also by the same argument can be made uniform. Therefore, by essentially the same proof as of Theorem 19, we can show that $\langle \widehat{C}, \widehat{R} \rangle$ is robust-CCA secure and omit a full proof.

Acknowledgments

We thank Stefano Tessaro for many helpful discussions on memory-hard functions and time-lock puzzles.

Huijia Lin and Pratik Soni were supported by NSF grants CNS-1528178, CNS-1514526, CNS-1652849 (CAREER), a Hellman Fellowship, the Defense Advanced Research Projects Agency (DARPA) and Army Research Office (ARO) under Contract No. W911NF-15-C-0236, and a subcontract No. 2017-002 through Galois.

Rafael Pass was Supported in part by an Alfred P. Sloan Fellowship, a Microsoft New Faculty Fellowship, NSF Awards CNS-1217821 and CCF-1214844, NSF CAREER Award CCF-0746990, AFOSR Award FA9550-08-1-0197, AFOSR YIP Award FA9550-10-1-0093, BSF Grant 2006317, and DARPA and AFRL under contract FA8750-11-2-0211.

The views and conclusions contained in this document are those of the authors and should not be interpreted as the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the US Government.

References

[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. In *43rd FOCS*, pages 345–355. IEEE Computer Society Press, November 2002.

[BDSK+18] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Huijia Lin, and Tal Malkin. Non-malleable codes against bounded polynomial time tampering. Cryptology ePrint Archive, Report 2018/1015, 2018. https://eprint.iacr.org/2018/1015.

[BF03] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[BGJ+16] Nir Bitansky, Shafi Goldwasser, Abhishek Jain, Omer Paneth, Vinod Vaikuntanathan, and Brent Waters. Time-lock puzzles from randomized encodings. In Madhu Sudan, editor, *ITCS 2016*, pages 345–356. ACM, January 2016.

[BHP17] Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou. Four round secure computation without setup. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 645–677. Springer, Heidelberg, November 2017.

[BL18] Nir Bitansky and Huijia Lin. One-message zero knowledge and non-malleable commitments. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography*, pages 209–234, Cham, 2018. Springer International Publishing.

[BN00] Dan Boneh and Moni Naor. Timed commitments. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 236–254. Springer, Heidelberg, August 2000.

[BOV03] Boaz Barak, Shien Jin Ong, and Salil P. Vadhan. Derandomization in cryptography. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 299–315. Springer, Heidelberg, August 2003.

[BP04] Boaz Barak and Rafael Pass. On the possibility of one-message weak zero-knowledge. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 121–132. Springer, Heidelberg, February 2004.

[BP15] Nir Bitansky and Omer Paneth. ZAPs and non-interactive witness indistinguishability from indistinguishability obfuscation. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 401–427. Springer, Heidelberg, March 2015.

[BY96] Mihir Bellare and Moti Yung. Certifying permutations: Noninteractive zero-knowledge based on any trapdoor permutation. *Journal of Cryptology*, 9(3):149–166, June 1996.

[CLP10] Ran Canetti, Huijia Lin, and Rafael Pass. Adaptive hardness and composable security in the plain model from standard assumptions. In *51st FOCS*, pages 541–550. IEEE Computer Society Press, October 2010.

[COSV16] Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Concurrent non-malleable commitments (and more) in 3 rounds. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 270–299. Springer, Heidelberg, August 2016.

[COSV17] Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Four-round concurrent non-malleable commitments from one-way functions. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 127–157. Springer, Heidelberg, August 2017.

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000.

[DN93] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 139–147. Springer, Heidelberg, August 1993.

[DN00] Cynthia Dwork and Moni Naor. Zaps and their applications. In *41st FOCS*, pages 283–293. IEEE Computer Society Press, November 2000.

[FLS90] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In *31st FOCS*, pages 308–317. IEEE Computer Society Press, October 1990.

[GKS16] Vipul Goyal, Dakshita Khurana, and Amit Sahai. Breaking the three round barrier for non-malleable commitments. In Irit Dinur, editor, *57th FOCS*, pages 21–30. IEEE Computer Society Press, October 2016.

[GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89, pages 25–32, New York, NY, USA, 1989. ACM.

[GLOV12] Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, and Ivan Visconti. Constructing non-malleable commitments: A black-box approach. In *53rd FOCS*, pages 51–60. IEEE Computer Society Press, October 2012.

[GLP+15] Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, and Amit Sahai. Round-efficient concurrently composable secure computation via a robust extraction lemma. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 260–289. Springer, Heidelberg, March 2015.

[GMPY11] Juan A. Garay, Philip D. MacKenzie, Manoj Prabhakaran, and Ke Yang. Resource fairness and composability of cryptographic protocols. *Journal of Cryptology*, 24(4):615–658, October 2011.

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, Heidelberg, August 2006.

[Goy11] Vipul Goyal. Constant round non-malleable protocols using one way functions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 695–704. ACM Press, June 2011.

[GPR16] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In Daniel Wichs and Yishay Mansour, editors, *48th ACM STOC*, pages 1128–1141. ACM Press, June 2016.

[JJ99] Markus Jakobsson and Ari Juels. Proofs of work and bread pudding protocols. In *Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security*, CMS '99, pages 258–272, Deventer, The Netherlands, The Netherlands, 1999. Kluwer, B.V.

[Khu17] Dakshita Khurana. Round optimal concurrent non-malleability from polynomial hardness. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part II*, volume 10678 of *LNCS*, pages 139–171. Springer, Heidelberg, November 2017.

[Kiy14] Susumu Kiyoshima. Round-efficient black-box construction of composable multi-party computation. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 351–368. Springer, Heidelberg, August 2014.

[KS17] Dakshita Khurana and Amit Sahai. How to achieve non-malleability in one or two rounds. In Chris Umans, editor, *58th FOCS*, pages 564–575. IEEE Computer Society Press, October 2017.

[LP09] Huijia Lin and Rafael Pass. Non-malleability amplification. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 189–198. ACM Press, May / June 2009.

[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 705–714. ACM Press, June 2011.

[LP12] Huijia Lin and Rafael Pass. Black-box constructions of composable protocols without set-up. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 461–478. Springer, Heidelberg, August 2012.

[LPV08] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. Concurrent non-malleable commitments from any one-way function. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 571–588. Springer, Heidelberg, March 2008.

[May93] Timothy May. Timed-release crypto. 1993.

[Nak12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. 2012.

[Pas13] Rafael Pass. Unprovable security of perfect NIZK and non-interactive non-malleable commitments. In Amit Sahai, editor, *TCC 2013*, volume 7785 of *LNCS*, pages 334–354. Springer, Heidelberg, March 2013.

[PPV08] Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan. Adaptive one-way functions and applications. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 57–74. Springer, Heidelberg, August 2008.

[PR05a] Rafael Pass and Alon Rosen. Concurrent non-malleable commitments. In *46th FOCS*, pages 563–572. IEEE Computer Society Press, October 2005.

[PR05b] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 533–542. ACM Press, May 2005.

[PW10] Rafael Pass and Hoeteck Wee. Constant-round non-malleable commitments from sub-exponential one-way functions. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 638–655. Springer, Heidelberg, May / June 2010.

[Rog06] Phillip Rogaway. Formalizing human ignorance. In Phong Q. Nguyen, editor, *Progress in Cryptology - VIETCRYPT 06*, volume 4341 of *LNCS*, pages 211–228. Springer, Heidelberg, September 2006.

[RSW96] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical report, Massachusetts Institute of Technology, Cambridge, MA, USA, 1996.

[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. In *51st FOCS*, pages 531–540. IEEE Computer Society Press, October 2010.

11 Appendix

11.1 Proof of Theorem 15

Proof. Recall that we want to show the following,

1. If $\langle \widehat{C}, \widehat{R} \rangle$ is $\mathcal{C}$-one-many non-malleable then it is $\mathcal{C}$-concurrent non-malleable.
2. If $\langle \widehat{C}, \widehat{R} \rangle$ is $\mathcal{C}$-one-many non-malleable w.r.t. extraction (by extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$) then it is $\mathcal{C}$-concurrent non-malleable w.r.t. extraction (by $\widehat{o\mathcal{E}_{\mathsf{NM}}}$).

We begin by proving the second implication, that is, $\mathcal{C}$-one-many non-malleability w.r.t. extraction implies $\mathcal{C}$-concurrent non-malleability w.r.t. extraction. Let us assume for contradiction that there exists a non-uniform adversary $A = \{A_n\}_{n\in\mathbb{N}} \in \mathcal{C}$ that participates in $m = \mathsf{poly}(n)$ concurrent interactions while sending/receiving commitments to $\alpha = \mathsf{poly}(n)$-bit values, a non-uniform distinugisher $D = \{D_n\}_{n\in\mathbb{N}} \in \mathcal{P}/\mathrm{poly}$, and a polynomial $p(\cdot)$ such that for infinitely many $n \in \mathbb{N}$,

$$\left|\mathsf{Pr}[D_n(\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 0))] - \mathsf{Pr}[D_n(\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1^n, 1))]\right| > \frac{1}{p(n)} \ . \tag{32}$$

Fix some generic n for which this happens. We next consider a sequence of hybrid MIM experiments $\{H_i\}_{0\le i\le m-1}$. In the honest MIM experiment $\mathsf{MIM}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(b)$ (for $b \in \{0,1\}$), A participates in m right interactions with $\widehat{R}$ and m left interactions with $\widehat{C}$. Recall that in all left interactions $i \in [m]$, A first chooses the identity id_i and challenge values (v_i^0, v_i^1), and interacts with $\widehat{C}$ to receive a commitment to value v_i^b with identity id_i. The hybrids H_i's we consider are identical to the MIM experiment $\mathsf{MIM}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(0)$ except that for all the left interactions $j \le i$ in H_i, A receives a commitment to the value v_j^1 instead of commitments to v_j^0. We let $\mathsf{emim}^{A}_{H_i}$ denote the random variable that describes the view of A and the values extracted from the right interactions in H_i by extractor $\widehat{o\mathcal{E}_{\mathsf{NM}}}$. It is easy to see that H_0 is identical to MIM experiment $\mathsf{MIM}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(0)$ (hence $\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(0) = \mathsf{emim}^{A}_{H_0}$) and H_m is identical to the MIM experiment $\mathsf{MIM}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1)$ (hence $\mathsf{emim}^{A}_{\langle \widehat{C},\widehat{R}\rangle}(1) = \mathsf{emim}^{A}_{H_m}$). By a standard hybrid argument, following Equation 32, there exists some $i \in \{0,\ldots,m-1\}$ such that,

$$\left|\mathsf{Pr}[D_n(\mathsf{emim}^{A}_{H_i})] - \mathsf{Pr}[D_n(\mathsf{emim}^{A}_{H_{i+1}})]\right| > \frac{1}{p(n)\cdot m} \ . \tag{33}$$

Given this, we construct a one-many non-uniform adversary $\widetilde{A} = \{\widetilde{A}_n\}_{n\in\mathbb{N}}$ for $\langle \widehat{C},\widehat{R}\rangle$ and a distinguisher $\widetilde{D} = \{\widetilde{D}_n\}_{n\in\mathbb{N}}$ that violate one-many non-malleability w.r.t. extraction of $\langle \widehat{C},\widehat{R}\rangle$ with advantage $1/(p(n)\cdot m(n))$. For $n \in \mathbb{N}$, $\widetilde{A}_n$ with index i (as defined above) hard-wired in it, participates in one left interaction with $\widehat{C}$ and m right interactions with $\widehat{R}$ and internally emulates an execution of H_i for A_n as follows: all right interactions of A_n are externally forwarded to $\widehat{R}$, the i-th left interaction of A_n is externally forwarded to $\widehat{C}$, and for all remaining left interactions $\widetilde{A}$ internally acts as a honest committer emulating hybrid H_i. More precisely, for the i-th left interaction, A_n forwards the identity id_i and values (v_i^0, v_i^1) sent by A_n to $\widehat{C}$ and receives a commitment to either v_i^0 or v_i^1, which $\widetilde{A}_n$ forwards to A_n as its i-th left commitment. The distinguisher $\widetilde{D}_n$ on input $\mathsf{emim}^{\widetilde{A}}_{\langle \widehat{C},\widehat{R}\rangle}(b)$, that is, the view $view$ of $\widetilde{A}_n$ and the values $u'_1,\ldots,u'_m$ extracted from the right interactions, runs the function $\mathsf{reconstruct}$ that reconstructs the view $view'$ of A in emulation by $\widetilde{A}$ and sets $\tilde{u}_k = u'_k$ iff A did not copy the identity of any of the m left interactions, and $\perp$ otherwise. $\mathsf{reconstruct}$ finally outputs $\tilde{u_1},\ldots,\tilde{u_m}, view'$. By construction it follows that,

$$\mathsf{reconstruct}(\mathsf{emim}^{\widetilde{A}}_{\langle \widehat{C},\widehat{R}\rangle}(0)) = \mathsf{emim}^{A}_{H_i} \ ; \ \mathsf{reconstruct}(\mathsf{emim}^{\widetilde{A}}_{\langle \widehat{C},\widehat{R}\rangle}(1)) = \mathsf{emim}^{A}_{H_{i+1}} \ .$$

The distinguisher $\widetilde{D}_n$ runs the distinguisher D_n on $\tilde{u}_1,\ldots,\tilde{u}_m, view'$ and outputs whatever D_n outputs. Then by Equation 33 it follows that the pair $(\widetilde{A},\widetilde{D})$ breaks the one-many non-malleability of $\langle \widehat{C},\widehat{R}\rangle$ w.r.t. extraction with advantage $1/(p(n)\cdot m(n))$. To arrive at a contradiction, we need to show that $\widetilde{A}$ and $\widetilde{D}$ belong to appropriate circuit classes. Firstly, note that $\widetilde{A}$ internally runs A and the rest of the computation can be done in $\mathsf{poly}(n)$-time. Therefore, the size/depth of $\widetilde{A}$ blows up only by an additive $\mathsf{poly}(n)$ factor over the size/depth of A. Secondly, $\widetilde{D}$ computes the

$\mathsf{reconstruct}$ function, runs D and the rest of the computation can be done in poly-time. Note that the $\mathsf{reconstruct}$ function is in fact computable in poly-time. Therefore, the size/depth of $\widetilde{A}$ blows up only by an additive $\mathsf{poly}(n)$ factor over the size/depth of A. Since $A \in \mathcal{C}$ and $D \in \mathcal{P}/\text{poly}$ and both $\mathcal{C}$ and $\mathcal{P}/\text{poly}$ are closed under composition with $\mathcal{P}/\text{poly}$, we conclude that $\widetilde{A} \in \mathcal{C}$ and $\widetilde{D} \in \mathcal{P}/\text{poly}$. This contradicts the one-many non-malleability w.r.t. extraction of $\langle \widehat{C}, \widehat{R} \rangle$.

The proof of concurrent non-malleability w.r.t. commitment follows syntactically from the proof of non-malleability w.r.t. extraction except that we consider the random variable $\mathsf{mim}^{A}_{\langle \widehat{C}, \widehat{R} \rangle}$ instead of $\mathsf{emim}^{A}_{\langle \widehat{C}, \widehat{R} \rangle}$. We skip the formal proof. $\square$