# Non-Interactive Non-Malleability from Quantum Supremacy

Yael Tauman Kalai
Microsoft Research, MIT
yael@microsoft.com

Dakshita Khurana
Microsoft Research
dakshita.khurana@microsoft.com

**Abstract**

We construct non-interactive non-malleable commitments without setup in the plain model, under well-studied assumptions.

First, we construct non-interactive non-malleable commitments with respect to commitment for $\epsilon \log\log n$ tags for a small constant $\epsilon > 0$, under the following assumptions:

1. Sub-exponential hardness of factoring or discrete log.
2. Quantum sub-exponential hardness of learning with errors (LWE).

Second, as our key technical contribution, we introduce a new tag amplification technique. We show how to convert any non-interactive non-malleable commitment with respect to commitment for $\epsilon \log\log n$ tags (for any constant $\epsilon > 0$) into a non-interactive non-malleable commitment with respect to replacement for $2^n$ tags. This part only assumes the existence of sub-exponentially secure non-interactive witness indistinguishable (NIWI) proofs, which can be based on sub-exponential security of the decisional linear assumption.

Interestingly, for the tag amplification technique, we crucially rely on the leakage lemma due to Gentry and Wichs (STOC 2011). For the construction of non-malleable commitments for $\epsilon \log\log n$ tags, we rely on quantum supremacy. This use of quantum supremacy in classical cryptography is novel, and we believe it will have future applications. We provide one such application to two-message witness indistinguishable (WI) arguments from (quantum) polynomial hardness assumptions.

# Contents

# 1 Introduction

Non-malleability, first introduced by Dolev, Dwork and Naor [DDN91] aims to counter the ubiquitous problem of man-in-the-middle (MIM) attacks on cryptographic protocols. A MIM adversary participates in two or more instantiations of a protocol, trying to use information obtained in one execution to breach security in the other protocol execution. A non-malleable protocol should ensure that such an adversary gains no advantage. A long-standing problem in this area has been to build non-malleable protocols, without any additional setup or rounds of interaction. In this paper, we develop techniques to address this question based on well-studied assumptions. We focus on a core non-malleable primitive – a commitment scheme.

**Non-interactive Commitments.** A non-interactive commitment scheme consists of a commitment algorithm, that on input a message $m$ and randomness $r$, outputs a string commitment to $m$, which is denoted by $\mathsf{com}(m;r)$[1]. A commitment scheme is required to be both binding and hiding. The (statistical) binding requirement asserts that a commitment cannot be opened to two different messages $m \neq m'$, namely, there do not exist $m \neq m'$ and randomness $r, r'$ such that $\mathsf{com}(m;r) = \mathsf{com}(m';r')$. The (computational) hiding property asserts that for any two messages, $m$ and $m'$ (of the same length), the distributions $\mathsf{com}(m)$ and $\mathsf{com}(m')$ are computationally indistinguishable. We note that one could also consider computational binding and statistical hiding, however such commitment schemes are known to require at least two rounds of interaction when dealing with non-uniform adversaries. The focus of this work is on the non-interactive setting.

**Non-interactive non-malleable commitments.** Loosely speaking, a commitment scheme is said to be non-malleable if no MIM adversary, given a commitment $\mathsf{com}(m)$, can efficiently generate a commitment $\mathsf{com}(m')$, such that the message $m'$ is related to the original message $m$.

Non-malleable commitments are among the core building blocks of various cryptographic protocols such as coin-flipping, secure auctions, electronic voting, general multi-party computation protocols, and non-malleable proof systems. Therefore, they have a direct impact on the round complexity of such protocols. For example, many constructions of concurrent MPC against Byzantine adversaries are bottlenecked by the round complexity of non-malleable commitments.

As such, there has been a long line of work on constructing non-malleable commitments in the plain model in as few rounds as possible (e.g [DDN91, Bar02, PR05a, PR08, LPV, PPV08, LP09, Wee10, PW10, LP, Goy11, GLOV12, GRRV14, GPR16, COSV16, COSV17, Khu17, LPS17, KS17]). So far, the only known constructions of non-interactive non-malleable commitments (without setup) are the ones by Pandey, Pass and Vaikuntanathan [PPV08], based on a strong non-falsifiable assumption, and Bitansky and Lin [BL18], based on a relatively new assumption about sub-exponential incompressible functions. We elaborate on these related works in Section 1.3.

Indeed, constructing non-interactive non-malleable commitment schemes (without setup) from standard assumptions, has been a long standing open problem and is the focus of this work.

Three primary flavours of non-malleability have been considered in the literature:

- **Non-malleability with respect to commitment.** Intuitively, non-malleability with respect to commitment, which is the strongest of the three definitions, requires that for any two messages $m_0, m_1 \in \{0,1\}^p$, the distributions $(\mathsf{Com}(m_0), \widetilde{m}_0)$ and $(\mathsf{Com}(m_1), \widetilde{m}_1)$ are computationally indistinguishable. Here $\widetilde{m}_b$ is the message committed to by the MIM given $\mathsf{Com}(m_b)$, and is set to $\perp$ if the adversary given $\mathsf{Com}(m_b)$ outputs $\widetilde{c}$ for which there do not exist any

[1] We will sometimes omit explicitly writing the randomness $r$.

$(\widetilde{m}, \widetilde{r})$ such that $\widetilde{c} = \mathsf{com}(\widetilde{m}; \widetilde{r})$. It was shown by [BFMR18] that in the case of non-interactive commitments, non-malleability w.r.t. commitment is equivalent to CCA-security.

- **Non-malleability with respect to replacement.** A weaker, yet natural, notion of malleability is non-malleability with respect to replacement [Goy11]. This requires that for any two messages $m_0, m_1 \in \{0,1\}^p$, the distributions $(\mathsf{Com}(m_0), \widetilde{m}_0)$ and $(\mathsf{Com}(m_1), \widetilde{m}_1)$ are indistinguishable *whenever* $\widetilde{m}_0, \widetilde{m}_1 \neq \perp$.[2] This is exactly like non-malleability with respect to commitment, except that the adversary is allowed to perform "selective abort" attacks, where the event that the adversary committed to an invalid message, is allowed to be correlated with the honest message. This guarantees that a man-in-the-middle adversary cannot commit to *valid* messages that are related to the message committed in an honest protocol. We observe that the proofs in [BFMR18] demonstrate that non-interactive non-malleability w.r.t. replacement is equivalent to a weaker form of CCA-security. We further elaborate upon this in Section 1.2.

- **Non-malleability with respect to opening.** This is an even weaker[3], yet natural notion, which requires that for any two messages $m_0, m_1$, the joint distribution of $(\mathsf{Com}(m_0), \widetilde{m}_0)$ and $(\mathsf{Com}(m_1), \widetilde{m}_1)$ are indistinguishable *whenever* $\widetilde{m}_0, \widetilde{m}_1 \neq \perp$, where $\widetilde{m}_b$ is the message opened by the MIM given $\mathsf{Com}(m_b)$.

This work focuses on the first two definitions. We also note that all non-malleable commitment schemes assume that parties have "tags" (or id's), and require non-malleability to hold whenever the adversary is trying to commit w.r.t. $\widetilde{\mathsf{tag}}$ that is different from an honest $\mathsf{tag}$. We differentiate between the following two settings:

- One-to-one setting, where the man-in-the-middle (MIM) gets a single committed message and generates a single commitment.

- Many-to-many (concurrent) setting, where the MIM receives many commitments and is allowed to generate many commitments. Here, the guarantee is that for any two sets of committed messages sent to the MIM, the joint distribution of these committed messages and the messages that the MIM commits to, are indistinguishable.

In this work, we focus on the one-to-one definition. But as a stepping stone, we define and construct many-to-many *same-tag* non-malleable commitments. This is similar to the many-to-many notion, except that it restricts the MIM to use the same tag in all commitments that he outputs.

### 1.1 Our Results

In this paper, we first construct non-malleable commitments w.r.t. commitment for $\epsilon \log\log n$ tags (for some small constant $\epsilon > 0$) in the many-to-many same-tag setting, based on well-studied hardness assumptions, which we elaborate on below. Then we present a general "tag amplification" compiler that converts any non-malleable commitment w.r.t. replacement with $\epsilon \log\log n$ tags in the many-to-many same tag setting, into a non-malleable commitment w.r.t. replacement with $2^n$ tags in the one-to-one setting, assuming sub-exponential NIWI (which can in turn be based on the sub-exponential decisional linear (DLIN) assumption).

For the first result, our contribution is primarily conceptual, and relies on using *quantum supremacy*. Our second result contains the bulk of the technical difficulty. In this part, we make a

[2] As earlier, $\widetilde{m}_b$ denotes the message committed to by the MIM given $\mathsf{Com}(m_b)$.

[3] Non-malleability w.r.t. replacement implies non-malleability w.r.t. opening, as defined by Goyal et al. [GKS16].

novel use of the leakage lemma due to Gentry and Wichs [GW11]. The use of the leakage lemma in this context is surprising, since a-priori the problem of non-malleability seems quite unrelated to leakage. In what follows, we state our results in more detail.

### 1.1.1 Non-interactive non-malleable commitments for $O(\log \log n)$ tags.

We construct non-interactive non-malleable commitments w.r.t. commitment for $\epsilon \log \log n$ tags (for a small constant $\epsilon > 0$) assuming:

- Sub-exponential hardness of factoring or discrete log.
- Sub-exponential hardness of learning with errors (LWE) or learning parity with noise (LPN) against quantum circuits.

More generally, we construct non-malleable commitments w.r.t. commitment for $\epsilon \log \log n$ tags from any sub-exponentially secure bit commitment for 2 tags (denoted by $\mathsf{com}_0$ and $\mathsf{com}_1$), for which the hiding property of $\mathsf{com}_0$ holds even given an oracle that breaks $\mathsf{com}_1$, and similarly the hiding property of $\mathsf{com}_1$ holds even given an oracle that breaks $\mathsf{com}_0$. Such commitments are known as *adaptive* or CCA-secure commitments [PPV08, LP12][4].

**Informal Theorem 1.** *Assuming the existence of sub-exponentially secure many-to-many CCA bit commitments for 2 tags, there exist many-to-many same-tag non-interactive non-malleable string commitments with respect to commitment for $\epsilon \log \log n$ tags (for a small constant $\epsilon > 0$).*

To achieve this, we rely on the leveraging technique of Pass and Wee [PW10] that allows us to construct, from any sub-exponentially secure non-interactive commitment, a series of $\epsilon \log \log n$ commitments, each harder than the previous one.

In Section 2.2, we give an overview of the proof of Informal Theorem 1. However, our main conceptual novelty in this part, which we describe next, is the idea of constructing an adaptive or parallel-CCA secure commitment scheme for 2 tags using *quantum supremacy*.

**Using Quantum Supremacy.** Loosely speaking, in order to construct an adaptive commitment for 2 tags, we need two axes of hardness: One axis in which $\mathsf{com}_0$ is harder than $\mathsf{com}_1$, and the other in which $\mathsf{com}_1$ is harder than $\mathsf{com}_0$.

We build such an axis by relying on quantum supremacy, which is the ability of quantum computers to solve problems (such as factoring) that are believed to be hard for classical computers. Namely, we construct two commitment algorithms $\mathsf{com}_0$ and $\mathsf{com}_1$ such that for quantum algorithms, breaking $\mathsf{com}_1$ is harder than breaking $\mathsf{com}_0$, and yet for classical algorithms, breaking $\mathsf{com}_0$ is harder than breaking $\mathsf{com}_1$.

This is achieved by instantiating $\mathsf{com}_1$ as a post-quantum secure commitment (such as one based on LWE or LPN [GHKW17]); and instantiating $\mathsf{com}_0$ as a post-quantum *insecure* commitment (such as one based on factoring or discrete log via Goldreich-Levin [Lev87]), albeit with a much larger security parameter. Now, given a BQP oracle, $\mathsf{com}_1$ is secure but $\mathsf{com}_0$ is not; at the same time, classical machines can break $\mathsf{com}_1$ faster than they can break $\mathsf{com}_0$. We prove the following claim:

**Informal Claim 1.** *Assuming sub-exponential hardness of factoring or discrete log, and sub-exponential quantum hardness of LWE or LPN, there exist sub-exponentially secure many-to-many CCA bit commitments for 2 tags.*

[4] We interpret these as CCA-secure commitments for the sake of simplcity of our proof, but in the non-interactive setting [BFMR18], these are equivalent to many-many non-malleable commitments w.r.t. commitment.

Combining this with Informal Theorem 1, we have:

**Informal Theorem 2.** *Assuming sub-exponential hardness of factoring or discrete log, and sub-exponential quantum hardness of LWE or LPN, there exist many-to-many same-tag non-interactive non-malleable commitments with respect to commitment for $\epsilon \log\log n$ tags, for a small constant $\epsilon > 0$.*

Prior to this work, obtaining non-interactive non-malleable commitments w.r.t. commitment, even for just two tags, required the non-standard assumption that there exist sub-exponential incompressible one-way functions, and either sub-exponentially secure time-lock puzzles or sub-exponentially secure one-way functions admitting hardness amplification exist [BL18]. The work of [LPS17] constructed non-interactive non-malleable commitments *w.r.t. extraction* (which is similar to w.r.t. replacement) for $O(\log\log n)$ tags assuming sub-exponentially secure time-lock puzzles or sub-exponentially secure one-way functions that admit hardness amplification [BL18] We show that non-interactive non-malleable commitments w.r.t. commitment for $\epsilon \log\log n$ tags (in fact, even parallel CCA commitments for 2 tags) can be constructed based on much more well-studied assumptions than previously known.

We believe that this idea of using quantum supremacy may have other applications in classical cryptography. In particular, the technique of complexity leveraging, which breaks hardness of one primitive while retaining hardness of another, is extensively used in cryptography. Whenever this technique is used, the resulting scheme needs to rely on super-polynomial (and often sub-exponential) hardness assumptions. We believe that in several such applications, the complexity leveraging technique can be replaced with quantum supremacy, thus converting such super-polynomial hardness assumptions to quantum polynomial hardness assumptions. For example, using our ideas, one can appropriately instantiate the protocols in [JKKR17] to obtain two-message witness indistinguishable protocols based on quantum-polynomial hardness of LWE, and polynomially hard one-way functions (such as those based on factoring or discrete log) that are invertible in BQP. We give details of this construction in Appendix A.

We also remark that one can substitute the assumption on sub-exponential quantum hardness of LWE with sub-exponentially secure time-lock puzzles [LPS17], or sub-exponentially secure one-way functions [BL18] admitting hardness amplification, to obtain (many-to-many) non-malleable commitments w.r.t. replacement for $\epsilon \log\log n$ tags.

### 1.1.2 Non-interactive Tag Amplification from NIWIs

Our more involved technical contribution is a non-interactive tag amplification technique that relies only on sub-exponentially secure non-interactive witness indistinguishable (NIWI) proofs.

**Informal Theorem 3** (Tag Amplification from NIWIs)**.** *Assuming many-to-many same-tag non-malleable commitments with respect to replacement for $\epsilon \log\log n$ tags (for an arbitrarily small constant $\epsilon > 0$) and sub-exponentially secure NIWIs, there exist non-interactive non-malleable commitments with respect to replacement for $2^n$ tags.*

We note that sub-exponentially secure NIWIs can be constructed assuming the sub-exponential hardness of the decisional linear problem [GOS12], or from derandomization assumptions [BOV07], or assuming indistinguishability obfuscation [BP15]. Interestingly, to prove this theorem, we crucially rely on the Gentry-Wichs leakage lemma [GW11]. We provide a high-level overview of this amplification technique, as well as its proof, in Section 2.1.

To summarize, assuming sub-exponential hardness of factoring or discrete log, as well as sub-exponential quantum hardness of LWE or LPN, there exist:

- Non-interactive non-malleable commitments with respect to commitment for $\epsilon \log \log n$ tags.
- Non-interactive non-malleable commitments with respect to replacement for $2^n$ tags, additionally assuming sub-exponentially secure NIWIs.

### 1.2 Applications and Directions for Future Work

As mentioned above, our final result (for $2^n$ tags) satisfies non-malleability w.r.t. replacement. In what follows, we motivate and give some additional perspectives on this notion.

- Non-malleable commitments wr.t. replacement imply the indistinguishability-based notion of non-malleable commitments w.r.t. opening, as defined in [CGM+16, GKS16]. Therefore, we obtain non-interactive non-malleable commitments w.r.t. opening from well-studied assumptions.

  **Informal Theorem 4.** *Assuming sub-exponential hardness of discrete log or factoring, sub-exponential quantum hardness of LWE or LPN, and sub-exponentially secure NIWIs, there exist non-interactive non-malleable commitments w.r.t. opening (for $2^n$ tags).*

- It was shown by [BFMR18] that the definitions of non-malleability w.r.t. commitment and (one-to-one) CCA-security are equivalent in the setting of non-interactive commitments. We observe that their proofs also imply equivalence between non-malleability w.r.t. replacement and a weaker notion of one-to-one CCA-security, where if the adversary queries the CCA oracle with a commitment to an invalid value, the oracle is allowed to respond with any arbitrary value of its choice.

- Non-interactive non-malleable commitments w.r.t. opening are known to be equivalent to block-wise non-malleable codes [CGM+16] with two blocks. Block-wise non-malleable codes are a strengthening of the notion of split-state non-malleable codes. Using our result, we obtain the first block-wise non-malleable codes that only require two blocks (or states), based on well-studied assumptions.

  **Informal Theorem 5.** *Assuming sub-exponential hardness of discrete log or factoring, sub-exponential quantum hardness of LWE or LPN, and sub-exponentially secure NIWIs, there exist 2-block blockwise non-malleable codes.*

- When restricted to adversaries that only output valid commitments, the notions of non-malleability w.r.t. replacement and non-malleability w.r.t. commitment are equivalent. Therefore, non-malleable commitments w.r.t. replacement can be combined with an appropriate ZK proof of validity of the commitment (as is implicit in [GRRV14, COSV16]) to obtain non-malleable commitments w.r.t. commitment. For instance, (sub-exponential) NIWI and (sub-exponential) keyless collision resistant hash functions against *uniform adversaries* are known to imply one-message zero-knowledge with soundness against uniform (sub-exponential time) adversaries [BP04, LPS17], and admitting a non-uniform simulator. Combining these with our non-malleable commitments w.r.t. replacement, we have the following theorem.

  **Informal Theorem 6.** *Assuming sub-exponential hardness of discrete log or factoring against non-uniform adversaries, sub-exponential quantum hardness of LWE or LPN against non-uniform adversaries, sub-exponentially secure keyless collision-resistant hash functions against uniform adversaries, and sub-exponentially secure NIWIs against uniform adversaries, there exist non-interactive non-malleable commitments w.r.t. commitment against uniform adversaries.*

Similarly, our commitment with can be appended with one-message ZK arguments of validity of the commitments, against any restricted class of adversaries, to yield non-malleable commitments w.r.t. commitment, against the same restricted classes of adversaries.

- Non-malleable commitments w.r.t. replacement are known to be sufficient for MPC [Goy11]. We believe that our constructions of non-malleable commitments w.r.t. replacement will help obtain constructions of two-message concurrent secure computation against malicious adversaries (with super-polynomial simulation) from well-studied assumptions. A detailed exploration is beyond the scope of this work.
- The recent works of [KY18, FF18] give constructions of non-malleable point obfuscation and non-malleable digital lockers from strong variants of the DDH assumption. We believe that our commitments will find applications to achieving non-malleability in context of witness encryption, obfuscation and many other inherently non-interactive primitives, based on well-studied assumptions.

### 1.3 Prior work

The work of [LPS17] constructed non-interactive non-malleable commitments w.r.t. commitment against a restricted class of *uniform* man-in-the-middle adversaries, assuming sub-exponentially secure time-lock puzzles, sub-exponential NIWI and sub-exponential collision-resistant hash functions against uniform adversaries. [BDK+18] in very recent independent work construct a significantly weaker object that they call non-interactive quasi-non-malleable commitments, based on well-studied assumptions. These commitments guarantee security against adversaries running in a-priori bounded polynomial time $O(n^c)$, but allow honest parties to run in longer (polynomial) time. These are used as a stepping stone in [BDK+18] to build non-malleable codes against bounded polynomial time tampering.

In this paper, our focus is on the non-interactive setting in the plain model against all polynomial-sized adversaries. In this setting, constructions of non-malleable commitments have remained elusive, except based on non-standard assumptions. In particular, prior to our work, there were only two known constructions, described below.

Pandey et al. [PPV08] constructed non-interactive concurrent non-malleable commitments w.r.t. commitment, starting from a non-falsifiable assumption, that already incorporates a strong form of non-malleability called *adaptive* injective one-way functions. Very recently, Bitansky and Lin [BL18] constructed concurrent non-interactive non-malleable commitments w.r.t. commitment, based on the (relatively new, non-standard) assumption that there exist sub-exponential incompressible functions, sub-exponentially secure NIWI proofs, and either sub-exponential injective one-way functions that admit hardness amplification or sub-exponential time-lock puzzles.

**Non-Interactive Tag Amplification.** Tag amplification has been extensively studied in the non-malleability literature (e.g. [DDN91, LP09, Wee10, LPS17, BL18]). Of these, only the recent work of [BL18] considers tag amplification in the non-interactive setting against general adversaries. [BL18] make a relatively non-standard assumption about the existence of sub-exponential incompressible one-way functions, in addition to assuming the existence of a sub-exponentially secure NIWI proofs.

Our tag amplification technique only assumes the existence of a sub-exponentially secure NIWI proof. However, while our tag amplification technique yields commitments that are non-malleable w.r.t. replacement, the one in [BL18] yields commitments that are (concurrent) non-malleable w.r.t. commitment.

## 2 Overview of Techniques

We now proceed to an informal overview of our techniques. We start by describing our key technical contribution: our tag amplification compiler. We then proceed to describe our new constructions of non-malleable commitments for small tags, which satisfy many-to-many same-tag non-malleability with respect to commitment.

### 2.1 Non-interactive Tag Amplification

Our starting point is the following basic idea. Start with a non-malleable commitment scheme $\mathsf{com}$ for tags in $[\alpha]$ where $\alpha \leq \mathsf{poly}(n)$, and obtain a scheme $\mathsf{Com}$ for tags in $\left[2^{\alpha/2}\right]$, as follows: To commit to a message $m$ with respect to a tag $T$, first compute $\{t_1, t_2, \ldots t_{\alpha/2}\}$, such that each $t_i = (i||T_i)$ where $T_i$ denotes the $i^{th}$ bit of $T$[5]. Let

$$\mathsf{Com}_T(m) \triangleq \{\mathsf{com}_{t_i}(m)\}_{i\in[\alpha/2]}.$$

Note that for any two tags $T = \{t_1, t_2, \ldots, t_{\alpha/2}\}$ and $\widetilde{T} = \{\widetilde{t}_1, \widetilde{t}_2, \ldots, \widetilde{t}_{\alpha/2}\}$ such that $\widetilde{T} \neq T$, there exists at least one index $i$ such that $\widetilde{t}_i \notin \{t_1, t_2, \ldots t_{\alpha/2}\}$. Therefore, if the underlying $\mathsf{com}$ is $\alpha/2$-to-1 non-malleable, then given $\mathsf{Com}_T(m) = \{\mathsf{com}_{t_i}(m)\}_{i\in[\alpha/2]}$, it should be hard to generate $\mathsf{com}_{\widetilde{t}_i}(m')$ for a related message $m'$. This seems to suggest that an adversary cannot generate a *valid* commitment $\mathsf{com}_{\widetilde{T}}(\widetilde{m})$ to a related message $\widetilde{m}$, i.e., that the resulting scheme is non-malleable w.r.t. replacement.

However, the security of this scheme completely breaks down even if the adversary receives *two commitments*. Specifically, an adversary that receives two commitments $\mathsf{Com}_T(m)$ and $\mathsf{Com}_{T'}(m)$ with different tags $T = \{t_1, t_2, \ldots, t_{\alpha/2}\}$ and $T' = \{t'_1, t'_2, \ldots, t'_{\alpha/2}\}$, can easily output $\mathsf{Com}_{\widetilde{T}}(m)$, where $\widetilde{T} = \{t_1, \ldots t_{\alpha/4}, t'_{\alpha/4+1}, \ldots t'_{\alpha_2}\}$. In other words, the resulting scheme *does not satisfy* many-to-1 non-malleability (or even 2-to-1 non-malleability), and is only non-malleable in the 1-to-1 setting.

Thus, using this idea we can go from $\eta \log\log n$ tags to $2^{\frac{\eta}{2}\log\log n} = \log^{\frac{\eta}{2}} n$ tags, but cannot continue further, since this compiler uses an underlying commitment which is many-to-one non-malleable (or more specifically, $\alpha/2$-to-1 non-malleable).

The blueprint in [KS17] describes how this problem can be solved using a NIZK, which requires the existence of a common random string (which we want to avoid). Namely, they show that if we append to the commitment $C = \{\mathsf{com}_{t_i}(m)\}_{i\in[\alpha/2]}$ a NIZK proof that all these $\alpha/2$ commitments $\mathsf{com}_{t_i}$ are to the same message $m$, then one can indeed prove that this resulting scheme is many-to-one non-malleable[6]. Instead, in this work, we rely on non-interactive proofs satisfying a weaker hiding property, i.e., witness indistinguishability[7]. This introduces several problems and bottlenecks that do not come up when using NIZKs. In particular, techniques in [KS17] rely on the reduction's ability to generate "simulated" proofs, a notion that is not applicable when using NIWIs. We discuss these barriers in further detail below.

#### 2.1.1 Tag Amplification using NIWIs: First Stab

While NIWI proofs have been extremely useful in a wide variety of cryptographic settings, they often become meaningless when trying to prove NP statements that have a single witness, such as

[5] Our actual encoding of $T$ to $\{t_1, t_2, \ldots t_{\alpha/2}\}$ is slightly more sophisticated, but achieves the same effect.

[6] To be precise, they need to rely on the fact that the NIZK is "more secure" than the underlying commitment scheme.

[7] As with NIZKs used in [KS17], we also require our NIWI to be more secure than the underlying commitment, which results in a sub-exponential assumption on the NIWI.

the one described above. Typically, NIWI proofs are only useful for statements that have at least two independent witnesses.

One can create a statement with two independent witnesses by repeating the blueprint twice in parallel. Namely, commit to a message $m$ by computing $C_1 = \{\mathsf{com}_{t_i}(m; r_{i,1})\}_{i\in[\alpha/2]}, C_2 = \{\mathsf{com}_{t_i}(m; r_{i,2})\}_{i\in[\alpha/2]}$ where $\{r_{i,b}\}_{i\in[\alpha/2],b\in\{0,1\}} \xleftarrow{\$} \{0,1\}^*$, and add a NIWI proving that all the commitments, in either $C_1$ or $C_2$, are to the same message.

Indeed, one can easily prove that if the underlying scheme for $\alpha$ tags is $(\alpha/2)$-to-1 non-malleable, then the resulting scheme is one-to-one non-malleable w.r.t. replacement[8].

Unfortunately, it is not clear if the resulting scheme satisfies even 2-to-1 non-malleability (w.r.t. replacement). Roughly speaking, the problem is as follows. For simplicity, consider a MIM that obtains commitments which are both commitments to $m_1$ or both to $m_2$, and tries to copy $m_1$ (or $m_2$). A natural approach to rule out such a MIM would be to rely on an intermediate hybrid, in which the MIM obtains a commitment to $(m_1, m_2)$.[9] Unfortunately, we have no way to use a hybrid argument to rule out a MIM that does the following:

- In the first hybrid, on input commitments to $(m_1, m_1)$, outputs a (valid) commitment to $m_1$.
- In the intermediate hybrid, on input commitments to $(m_1, m_2)$, outputs an invalid commitment where the first repetition in the MIM's commitment consists of all commitments to $m_1$, and the second repetition consists of all commitments to $m_2$, and these commitments are accompanied with an accepting NIWI proof.
- In the final hybrid, on input commitments to $(m_2, m_2)$, outputs a (valid) commitment to $m_2$.

The problem is that neither of the two pairs of adjacent hybrids can be used to get a contradiction to the one-to-one non-malleability, because neither are violating the non-malleability criterium w.r.t. replacement[10].

However, as we already noted above, many-to-one non-malleability is essential if we want to use the compiler again. In fact, it may seem like the NIWIs were not useful at all, since we could get one-to-one non-malleability even for the basic scheme described at the beginning of this overview, which did not require any NIWI (or NIZK). While at first, this approach seems to be inherently problematic, we will now describe how we can nevertheless rely on NIWIs to obtain our desired compiler, as follows

### 2.1.2 Overview of Our Compiler

Our idea is to have each commitment consist of at least $(\ell + 1)$ repetitions (as opposed to only 2), where $\ell$ is the number of commitments that the adversary can receive (on the left). Additionally, the committer is required to provide a NIWI proof that in all but one of these parallel executions, the messages committed across all $\alpha/2$ tags are identical. That is, in a valid commitment, all $(\ell+1)$ repetitions commit to the same message.

Now, when we perform the same hybrid argument as above where we change one left commitment in each hybrid, we have the following invariant: in all but one repetition, by the soundness of the NIWI, the messages committed by the MIM are identical for all tags. This helps us argue

[8] On the other hand, if we used a NIZK, the resulting scheme would be many-to-1 non-malleable w.r.t. commitment. Obtaining non-malleability w.r.t. replacement appears to be inherent unless one relies on NIZKs (and a CRS).

[9] This is the standard approach used in all previous work on this topic.

[10] This problem can be avoided by relying on NIZKs which would prevent the MIM from behaving as in the intermediate hybrid. However, we cannot rely on NIZKs because they require a CRS.

that the MIM is forced to change the message in *at most one repetition in every hybrid.* We give a more detailed explanation in Section 2.1.3.

Since there are $(\ell + 1)$ repetitions and only $\ell$ hybrids, we then deduce that messages in at least one repetition must remain unchanged at the end of *all* $\ell$ *hybrids*[11]. Therefore, no adversary can commit to a *valid* message that is related to the messages committed to in the left executions.

We show that this compiler works even if the underlying scheme is non-malleable w.r.t. replacement (as opposed to being non-malleable w.r.t. commitment). However, there is a loss in parameters when applying this compiler, i.e., the compiler converts any $\ell$-to-$z$ non-malleable commitment w.r.t. replacement into an $\ell'$-to-$z'$ non-malleable commitment w.r.t. replacement, where $\ell'$ and $z'$ are smaller than $\ell$ and $z$. We do not discuss exact parameter constraints here, but refer the reader to Theorem 2 for details.

**Technical Bottlenecks.** The intuition above seems to imply that the adversary cannot convert a commitment to $m$ to a commitment to a related message $m'$. However, to formally prove that this construction satisfies the definition of non-malleability w.r.t. replacement[12], we need to argue that there exists an (inefficient) extractor $\mathcal{V}_{\mathsf{Real}}(\tau_{\mathsf{Real}})$ corresponding to the transcript of a "real" experiment with honest messages $(m_1, \ldots m_\ell)$, and an (inefficient) extractor $\mathcal{V}_{\mathsf{Ideal}}(\tau_{\mathsf{Ideal}})$ corresponding to the transcript of an "ideal" experiment with honest messages $(0, 0, \ldots, 0)$, such that the joint distribution of the view of the MIM in the real experiment and the values output by $\mathcal{V}_{\mathsf{Real}}$, is indistinguishable from the joint distribution of the view of the MIM in the ideal experiment and the values output by $\mathcal{V}_{\mathsf{Ideal}}$. Furthermore, whenever the MIM generates a "valid" commitment $\widetilde{c}$ to a message $\widetilde{m}$ in either the real or ideal experiment, $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ are required to output $\widetilde{m}$. Therefore, we need to define distributions $\mathcal{V}_{\mathsf{Real}}(\tau_{\mathsf{Real}})$ and $\mathcal{V}_{\mathsf{Ideal}}(\tau_{\mathsf{Ideal}})$, and ensure that they are indistinguishable.

It is tempting to define $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ to output $\widetilde{M}$ corresponding to the MIM's commitment string $\widetilde{c}$, if there exists $\widetilde{r}$ such that $\widetilde{c} = \mathsf{com}(\widetilde{M}, \widetilde{r})$, and otherwise output $\perp$. However, as observed by the intuition above, these distributions will not necessarily be indistinguishable.[13] Namely, the adversary may generate valid commitments when given commitments to $m$ and commit to $\perp$ when given commitments to $0$.

Intuitively, to make these distributions indistinguishable, we will introduce some "slack", and sometimes output a valid message even though the adversary did not commit to a "perfectly valid" message. The question is the following: Suppose that the adversary outputs a commitment that is "close to" being a valid commitment to a message $\widetilde{m}$. Should the extractors $\mathcal{V}_{\mathsf{Real}}$ or $\mathcal{V}_{\mathsf{Ideal}}$ output $\widetilde{m}$ or output $\perp$? This is precisely where the leakage lemma of Gentry and Wichs [GW11] plays a crucial role. This decision of whether to output $\widetilde{m}$ or output $\perp$ will be dictated by a leakage function. We will need to "carry over" this leakage function across hybrids by relying on the leakage lemma. The proof of non-malleability of this amplification step is the primary technical contribution of our paper. There are many additional technical subtleties that were not discussed. For instance, in order to argue that the compiler can be applied several times, we work with a strong variant of non-malleability w.r.t. replacement (which only strengthens our final result). We give a more detailed protocol description in Section 2.1.3, and refer the reader to Section 5 for details of the proof.

[11] To simplify our proof, we rely on $10\ell$ repetitions (instead of $\ell + 1$) repetitions, to ensure that the messages in *most* repetitions remain unchanged.

[12] We refer the reader to Definition 3 for a one-to-one definition, and Definition 2 for a many-to-many definition.

[13] We note that these distributions are indeed indistinguishable if the adversary always generates valid commitments.

**Putting Things Together.** We now describe how we use this compiler to obtain our final result, i.e. non-malleable commitments for $2^n$ tags. Our starting point is our scheme for $\eta \log\log n$ tags which is many-to-many same-tag non-malleable w.r.t. commitment, and in particular is many-to-many same-tag non-malleable w.r.t. replacement (we give an overview of this scheme in Section 2.2). We will use the compiler above *three times*: First we convert the scheme for $\eta \log\log n$ tags into a scheme for $\log^{\eta/2}(n)$ tags, then we convert the resulting scheme for $\log^{\eta/2}(n)$ tags into a scheme for $2^{\log^{\epsilon} n}$ tags (for a small constant $\epsilon > 0$). We apply the compiler one final time to the scheme for $2^{\log^{\epsilon} n}$ tags to get a scheme for $\omega(n^{\log n})$ tags.

We note that it is not clear that we can run the compiler on itself many times, since every time we run the compiler, there is a loss in parameters. However, we set parameters carefully so that this nevertheless goes through.

To go from $n^{\log n}$ tags to $2^n$ tags, we use the (standard) idea of relying on sub-exponentially secure signatures. Specifically, to commit to a message $m$ with tag $T \in [2^n]$, we generate a random pair $sk, vk$ of signing and verification keys for the underlying scheme, where the verification key is of length $\log^2 n$ bits. We use $vk$ as our "small" tag for the non-malleable commitment, and sign the larger tag $T \in [2^n]$ with $sk$. The security of this construction follows by the (sub-exponential) unforgeability of the underlying signature scheme. We refer the reader to Section 6 for more details.

### 2.1.3 More Detailed Protocol Description

Finally, to help the reader navigate our tag amplification protocol, we now give a slightly more detailed description of our protocol, and the intuition for non-malleability. As mentioned above, to commit to message $m$ with tag $T = \{t_1, t_2, \ldots t_{\alpha/2}\}$, the committer commits to the message $k = 10\ell$ times in parallel with tags $\{t_1, t_2, \ldots t_{\alpha/2}\}$, using fresh randomness each time.

Our protocol is described informally in Figure 1. Note that the protocol is not many-to-many, because as explained above, the size of the resulting commitment grows linearly with $\ell$.

Roughly, we prove that if our underlying commitment scheme com is many-to-$z$ non-malleable w.r.t. replacement, and is secure against $2^y$-sized adversaries, then the resulting scheme is $\ell$-to-$y$ non-malleable w.r.t. replacement, for any $y$ and $\ell$ such that $\ell \cdot y < \frac{z}{10}$. We require the NIWI to be WI against $\mathsf{poly}(T)$-time adversaries, where $T$ is the time required to brute-force break com.

**Intuition for Non-Malleability.** For simplicity, let us consider a MIM adversary that on input $\ell$ commitments, with corresponding tags $T_1, T_2, \ldots T_\ell$, outputs a single commitment $\widetilde{c}$ with tag $\widetilde{T}$ (in our actual proof, the MIM is allowed to output multiple commitments, albeit using the same tag).

We need to argue that the MIM on input $\ell$ commitments to messages $m_1, \ldots, m_\ell$ cannot output a *valid* commitment to a related message $\widetilde{m}$. As eluded to earlier, this is done via a hybrid argument. Let us suppose for contradiction that on input commitments to $m_1, \ldots, m_\ell$, the adversary outputs a valid commitment to $\widetilde{m}$.

We consider a hybrid where the first honest commitment (on the left) is generated as a commitment to $0$ (but the rest are commitments to $m_2, \ldots m_\ell$). Letting $T_1 := \{t_{1,1}, t_{1,2}, \ldots t_{1,\alpha/2}\}$, one can argue that the joint distribution of the message $\widetilde{m}$ committed by the MIM using small tag $\widetilde{t_1} \notin \{t_{1,1}, t_{1,2}, \ldots t_{1,\alpha/2}\}$ in all $k$ repetitions, cannot change. This follows from the many-to-$z$ non-malleability with respect to commitment of com for $z \geq k$ (and relying on the fact that NIWI is hard against $\mathsf{poly}(T)$-time adversaries).

Furthermore, by the soundness of the MIM's NIWI, this implies that the MIM continues to commit to $\widetilde{m}$ in at least $(k-1)$ of his repetitions. This implies that the MIM continues to commit

**Parameters:** Set $k = 10\ell$.
**Committer Input:** Message $M \in \{0,1\}^{p(n)}$, and tag $\{t_1, t_2, \ldots t_{\alpha/2}\}$.

**Commit Stage:**

1. **Committer Message.**

   - For every $\lambda \in [\alpha/2]$ and every $j \in [k]$, sample randomness $r_{\lambda,j} \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$ and compute $C_{\lambda,j} = \mathsf{com}_{t_\lambda}(M; r_{\lambda,j})$.
   - Use witness $J = [k-1], \{M, r_{\lambda,j}\}_{\lambda \in [t/2], j \in J}$ to compute a NIWI proof $\Pi$ that there exists $J \subseteq [k]$ of size at least $(k-1)$, such that the following is true:
     For every $j \in J$, $\exists M_j$, $\{r_{\lambda,j}\}_{\lambda \in [\alpha/2]}$ so that $\{C_{\lambda,j} = \mathsf{com}_{t_\lambda}(M_j; r_{\lambda,j})\}_{\lambda \in [\alpha/2]}$.
   - Send to the receiver the message

     $$(\mathsf{tag}, \{(C_{\lambda,j}, t_\lambda)\}_{\lambda \in [t/2], j \in [k]}, \Pi)$$

   - **Receiver Acceptance.** Accept the comitment if and only if the proof $\Pi$ verifies.

**Reveal Stage:** The committer sends $M$ and $\{r_{\lambda,j}\}_{\lambda \in [t/2], \lambda \in [k]}$ to the receiver.

**Receiver Output:** The receiver accepts the decommitment if all $k \cdot \alpha/2$ are valid commitments to $M$.

Figure 1: Round-Preserving Tag Amplification

to $\widetilde{m}$ in least $(k-1)$ of the repetitions, *for every tag*. Using a similar argument to the one above, one can argue that on input $\ell$ commitments to messages $0, 0, m_3, \ldots, m_\ell$ (i.e., with the first two messages replaced by 0), the MIM continues to commit to $\widetilde{m}$ in at least $(k-2)$ repetitions, for every tag.

Continuing this way, we observe that the MIM continues to commit to $\widetilde{m}$ in at least $(k-\ell)$ repetitions, with respect to every tag, on input $\ell$ commitments to messages $(0, 0, \ldots, 0)$. Therefore on input $(0, 0, \ldots 0)$, the MIM either continues to commit to $\widetilde{m}$ or commits to $\perp$, and therefore, $\widetilde{m}$ must be unrelated to $m$. This is the key intuition for the security of our scheme.

As explained above, the actual analysis of indistinguishability of the *joint distribution* of the protocol transcript and messages committed by the MIM is quite involved, and requires multiple careful applications to the leakage lemma [GW11]. We refer the reader to Section 5 for details.

### 2.2 Non-Malleable Commitments with respect to Commitment for $\epsilon \log\log n$ Tags

To conclude this overview, we give a brief description of how we build a non-malleable commitment for $\epsilon \log\log n$ tags, where $\epsilon > 0$ is a small constant, from sub-exponential adaptive commitments for two tags[14]. This uses ideas similar to those in [LPS17, KS17].

Assume the existence of adaptive commitments $\mathsf{com}_0, \mathsf{com}_1$, and oracles $\mathcal{O}_0, \mathcal{O}_1$ such that $\mathsf{com}_0$ is *sub-exponentially* hard to invert given oracle $\mathcal{O}_1$, but $\mathsf{com}_1$ is invertible in the presence of $\mathcal{O}_1$. Similarly, $\mathsf{com}_1$ is *sub-exponentially* hard to invert given oracle $\mathcal{O}_0$, but $\mathsf{com}_0$ is invertible in the presence of $\mathcal{O}_0$.

[14]Recall that we build adaptive commitments for two tags using quantum supremacy, as discussed in Section 1.1. We refer the reader to Section 4.2 for further details.

We rely on a technique of Pass and Wee [PW10] to show that from any such adaptive commitments, one can derive a sequence of (bit) commitments $\{\mathsf{com}_{d,i}\}_{d\in\{0,1\},i\in[\zeta]}$, where $\zeta = \epsilon \log\log n$ for a small constant $0 < \epsilon < 1$, and where

$$\mathsf{com}_{d,i} : \{0,1\} \times \{0,1\}^{\ell_{d,i}(n)} \to \{0,1\}^*$$

such that for each $d \in \{0,1\}$,

$$\ell_{d,1} = \omega(\log n) < \ell_{d,2} < \ldots < \ell_{d,\zeta-1} < \ell_{d,\zeta} \triangleq n$$

and for every $i, j, k \in [\zeta]$ for which $k > i$, inverting $\mathsf{com}_{d,k}$ relative to the oracle $\mathcal{O}_{1-d}$ requires more time than jointly inverting $\mathsf{com}_{d,i}$ and $\mathsf{com}_{1-d,j}$, relative to the oracle $\mathcal{O}_{1-d}$.

In order to commit to a bit $b$ with $\mathsf{tag} \in [\zeta]$, the committer first XOR secret shares bit $b$ to obtain two shares $b_1$ and $b_2$. The commitment to $b$ simply consists of $\left(\mathsf{com}_{0,\mathsf{tag}}(b_1), \mathsf{com}_{1,\zeta-\mathsf{tag}}(b_2)\right)$.

**Analysis.** Suppose there exists a MIM adversary that on input a commitment to bit $b$ with respect to tag tag, commits to a related bit $b'$ with respect to $\widetilde{\mathsf{tag}} \neq \mathsf{tag}$. We have the following possibilities:

- If $\mathsf{tag} > \widetilde{\mathsf{tag}}$, then breaking $\mathsf{com}_{0,\mathsf{tag}}$ relative to oracle $\mathcal{O}_1$ is harder than jointly breaking $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$ and $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$ relative to $\mathcal{O}_1$.
- If $\mathsf{tag} < \widetilde{\mathsf{tag}}$, then breaking $\mathsf{com}_{1,\zeta-\mathsf{tag}}$ relative to $\mathcal{O}_0$ is harder than jointly breaking $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$ and $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$ relative to $\mathcal{O}_0$.

In the first case, we extract the bit $b'$ committed by the MIM by jointly breaking $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$ and $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$ relative to $\mathcal{O}_1$, and if $b'$ is related to $b$, we get a contradiction to the hardness of breaking $\mathsf{com}_{0,\mathsf{tag}}$ relative to $\mathcal{O}_1$. We can use a similar argument in the second case.

We also observe that we can allow the MIM to generate an arbitrary number of commitments on the right with the same $\widetilde{\mathsf{tag}}$, and rely on the same assumptions to argue that the joint distribution of bits committed by the MIM (in many right commitments) remains independent of the honest bit. This gives us many-to-many same tag non-malleable commitments with respect to commitment for $\epsilon \log\log n$ tags. For simplicity, we only focused on bit commitments in this overview. However it is easy to extend this construction to obtain string commitments for $\epsilon \log\log n$ tags, based on sub-exponential adaptive bit commitments for two tags. We give a formal construction and proof in Section 4.1.

# 3 Definitions

Let $n$ denote the security parameter. In all our definitions, the input message to the commitment scheme will be sampled from $\{0,1\}^p$ for a polynomially bounded function $p = p$.

For any $T = T(n)$, we use $\mathcal{X} \approx_{\mathsf{poly}(T(n))} \mathcal{Y}$ to denote two distributions such that for every $(T(n))^{O(1)}$-size distinguisher $\mathcal{D}$,

$$\Pr[\mathcal{D}(x) = 1 | x \xleftarrow{\$} \mathcal{X}] - \Pr[\mathcal{D}(x) = 1 | x \xleftarrow{\$} \mathcal{Y}] = \mathsf{negl}(n).$$

We denote by $\mathcal{X} \approx \mathcal{Y}$, the event that $\mathcal{X} \approx_{\mathsf{poly}(n)} \mathcal{Y}$.

### 3.1 Non-Malleable Commitments w.r.t. Replacement

In this section, we present the main definition of non-malleability that we achieve, which is known as *non-malleability w.r.t. replacement* ( [Goy11]). This definition is weaker than the original definition of non-malleability, which is known as *non-malleability with respect to commitment* (and is formally defined in Section 3.2).

Non-malleability considers a man-in-the-middle that receives a commitment to a message $m \in \{0,1\}^p$ and generates a new commitment $\widetilde{c}$. We say that the man-in-the-middle commits to $\perp$ if there does not exist any $(\widetilde{m}, \widetilde{r})$ such that $\widetilde{c} = \mathsf{com}(\widetilde{m}; \widetilde{r})$. Intuitively, the definition of non-malleability with respect to commitment requires that for any two messages $m_0, m_1 \in \{0,1\}^p$, the joint distributions of $(\mathsf{Com}(m_0), \widetilde{m}_0)$ and $(\mathsf{Com}(m_1), \widetilde{m}_1)$ are indistinguishable, where $\widetilde{m}_b$ is the message committed to by the MIM given $\mathsf{Com}(m_b)$. The definition of non-malleability w.r.t. replacement (that we achieve) intuitively requires this to hold only conditioned on $\widetilde{m}_0, \widetilde{m}_1 \neq \perp$.

We emphasize that we consider the case where the MIM gets a single committed message and generates a single commitment. This is known as the "one-to-one" definition. A stronger definition is the "many-to-many" definition (also known as concurrent non-malleability), where the MIM receives many commitments and is allowed to generate many commitments, and the guarantee is that for any two sets of messages committed to and sent to the MIM, the joint distribution of these commitments and the messages committed to by the MIM, are indistinguishable.

**Definition 1 (Non-Malleable Commitments w.r.t. Replacement).** *A non-interactive non-malleable (one-to-one) string commitment scheme with $N$ tags consists of a probabilistic poly-time algorithm $\mathcal{C}$, that takes as input a message $m \in \{0,1\}^p$, randomness $r \in \{0,1\}^{\mathsf{poly}(n)}$, and a $\mathsf{tag} \in [N]$, and outputs a commitment $\mathsf{com}_{\mathsf{tag}}(m; r)$. It is said to be non-malleable w.r.t. replacement if the following two properties hold:*

1. **Statistical binding.** *There do not exist $m_0, m_1 \in \{0,1\}^p$, $r_0, r_1 \in \{0,1\}^{\mathsf{poly}(n)}$ and $\mathsf{tag}_0, \mathsf{tag}_1 \in [N]$ such that $m_0 \neq m_1$ and $\mathsf{com}_{\mathsf{tag}_0}(m_0; r_0) = \mathsf{com}_{\mathsf{tag}_1}(m_1; r_1)$.*

2. **One-to-One Non-malleability.** *For any poly-size adversary $\mathcal{A}$, any $m \in \{0,1\}^p$ and any $\mathsf{tag} \in [N]$, there exist (possibly inefficient) functions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ such that the following holds:*

   (a) *Sample $r \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$ and set $c = \mathsf{com}_{\mathsf{tag}}(m; r)$. Let $(\widetilde{c}, z) = \mathcal{A}(c)$. If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}\}$, $\widetilde{M} \in \{0,1\}^{p(n)}$ and $\widetilde{r} \in \{0,1\}^{\mathsf{poly}(n)}$ such that $\widetilde{c} = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}; \widetilde{r})$ then $\widetilde{m} = \widetilde{M}$, otherwise no restrictions are placed on $\widetilde{m}$. We require that*

$$\Pr[\mathcal{V}_{\mathsf{Real}}(c, \widetilde{c}) = \widetilde{m}] = 1 - \mathsf{negl}(n).$$

   (b) *Sample $r_{\mathsf{Ideal}} \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$ and set $c_{\mathsf{Ideal}} = \mathsf{com}_{\mathsf{tag}}(0^p; r_{\mathsf{Ideal}})$. Let $(\widetilde{c}_{\mathsf{Ideal}}, z_{\mathsf{Ideal}}) = \mathcal{A}(c_{\mathsf{Ideal}})$. If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}\}$, $\widetilde{M}_{\mathsf{Ideal}} \in \{0,1\}^{p(n)}$ and $\widetilde{r}_{\mathsf{Ideal}} \in \{0,1\}^{\mathsf{poly}(n)}$ such that $\widetilde{c}_{\mathsf{Ideal}} = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_{\mathsf{Ideal}}; \widetilde{r}_{\mathsf{Ideal}})$ then $\widetilde{m}_{\mathsf{Ideal}} = \widetilde{M}_{\mathsf{Ideal}}$, otherwise no restrictions are placed on $\widetilde{m}_{\mathsf{Ideal}}$. We require that*

$$\Pr[\mathcal{V}_{\mathsf{Ideal}}(c_{\mathsf{Ideal}}, \widetilde{c}_{\mathsf{Ideal}}) = \widetilde{m}_{\mathsf{Ideal}}] = 1 - \mathsf{negl}(n).$$

   (c) *We require:*

$$\left(c, \widetilde{c}, z, \mathcal{V}_{\mathsf{Real}}(c, \widetilde{c})\right) \approx_c \left(c_{\mathsf{Ideal}}, \widetilde{c}_{\mathsf{Ideal}}, z_{\mathsf{Ideal}}, \mathcal{V}_{\mathsf{Ideal}}(c_{\mathsf{Ideal}}, \widetilde{c}_{\mathsf{Ideal}})\right).$$

   *over the randomness of sampling $r, r_{\mathsf{Ideal}}$*[15].

[15] Note that this definition explicitly considers auxiliary information $z$, but is equivalent to one that does not consider $z$. We explicitly consider $z$ for convenience.

We next present an (intermediate) security definition that we use as a stepping stone to achieve our main result. This is a many-to-many version of Definition 1, that restricts the adversary to use the same tag in all commitments that he outputs.

**Definition 2 ($\ell$-to-$y$ Same-tag Non-malleable Commitments w.r.t. Replacement).** *A non-interactive non-malleable commitment scheme with $N$ tags consists of a probabilistic poly-time algorithm $\mathcal{C}$, that takes as input a message $m \in \{0,1\}^p$, randomness $r \in \{0,1\}^{\mathsf{poly}(n)}$, and a $\mathsf{tag} \in [N]$, and outputs a commitment $\mathsf{com}_{\mathsf{tag}}(m;r)$. It is said to be $\ell$-to-$y$ same-tag non-malleable w.r.t. replacement for polynomials $\ell(\cdot)$ and $y(\cdot)$, if the following two properties hold:*

1. **Statistical binding.** *There do not exist $m_0, m_1 \in \{0,1\}^p$, $r_0, r_1 \in \{0,1\}^{\mathsf{poly}(n)}$ and $\mathsf{tag}_0, \mathsf{tag}_1 \in [N]$ such that $m_0 \neq m_1$ and $\mathsf{com}_{\mathsf{tag}_0}(m_0;r_0) = \mathsf{com}_{\mathsf{tag}_1}(m_1;r_1)$.*

2. **$\ell$-to-$y$ Non-malleability.** *For any poly-size adversary $\mathcal{A}$, any $m_1, \ldots, m_\ell \in \{0,1\}^p$, and any $\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell \in [N]$, there exist (possibly inefficient) functions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ such that the following holds:*

   *(a) Sample $r_1, \ldots, r_\ell \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$, set $c_i = \mathsf{com}_{\mathsf{tag}_i}(m_i;r_i)$ for every $i \in [\ell]$, and let $(\widetilde{c}_1, \ldots, \widetilde{c}_y, z) = \mathcal{A}(c_1, \ldots, c_\ell)$.*
   *If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i\in[\ell]}$ such that $\widetilde{c}_1, \ldots \widetilde{c}_y$ all use $\widetilde{\mathsf{tag}}$, then continue. Otherwise set $(\widetilde{m}_1, \ldots \widetilde{m}_n) = \mathsf{abort}$.*
   *For each $i \in [y]$, if there exists $\widetilde{M}_i \in \{0,1\}^p$ and $\widetilde{r}_i \in \{0,1\}^{\mathsf{poly}(n)}$ for which $\widetilde{c}_i = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_i;\widetilde{r}_i)$, set $\widetilde{m}_i = \widetilde{M}_i$, and otherwise no restrictions are placed on $\widetilde{m}_i$. We require that*

$$\Pr[\mathcal{V}_{\mathsf{Real}}(c_1, \ldots, c_\ell, \widetilde{c}_1, \ldots \widetilde{c}_y) = (\widetilde{m}_1, \ldots, \widetilde{m}_y)] = 1 - \mathsf{negl}(n)$$

   *(b) Sample $r_{\mathsf{Ideal},1}, \ldots, r_{\mathsf{Ideal},\ell} \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$, set $c_{\mathsf{Ideal},i} = \mathsf{com}_{\mathsf{tag}_i}(0^p; r_{\mathsf{Ideal},i})$ for every $i \in [\ell]$, and let $(\widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},y}, z_{\mathsf{Ideal}}) = \mathcal{A}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell})$.*
   *If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i\in[\ell]}$ such that $\widetilde{c}_{\mathsf{Ideal},1}, \ldots \widetilde{c}_{\mathsf{Ideal},y}$ all use $\widetilde{\mathsf{tag}}$, then continue. Otherwise set $(\widetilde{m}_{\mathsf{Ideal},1}, \ldots \widetilde{m}_{\mathsf{Ideal},n}) = \mathsf{abort}$.*
   *For each $i \in [y]$, if there exists $\widetilde{M}_{\mathsf{Ideal},i} \in \{0,1\}^p$ and $\widetilde{r}_{\mathsf{Ideal},i} \in \{0,1\}^{\mathsf{poly}(n)}$ for which $\widetilde{c}_{\mathsf{Ideal},i} = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_{\mathsf{Ideal},i}; \widetilde{r}_{\mathsf{Ideal},i})$, set $\widetilde{m}_{\mathsf{Ideal},i} = \widetilde{M}_{\mathsf{Ideal},i}$, and otherwise no restrictions are placed on $\widetilde{m}_{\mathsf{Ideal},i}$. We require that*

$$\Pr[\mathcal{V}_{\mathsf{Ideal}}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell}, \widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},y}) = (\widetilde{m}_{\mathsf{Ideal},1}, \ldots, \widetilde{m}_{\mathsf{Ideal},y})] = 1 - \mathsf{negl}(n)$$

   *(c) We require:*

$$\big((c_1, \ldots c_\ell), (\widetilde{c}_1, \ldots \widetilde{c}_y), z, \mathcal{V}_{\mathsf{Real}}(c_1, \ldots, c_\ell.\widetilde{c}_1, \ldots \widetilde{c}_y)\big) \approx_c$$
$$\big((c_{\mathsf{Ideal},1}, \ldots c_{\mathsf{Ideal},\ell}), (\widetilde{c}_{\mathsf{Ideal},1}, \ldots \widetilde{c}_{\mathsf{Ideal},y}), z_{\mathsf{Ideal}}, \mathcal{V}_{\mathsf{Ideal}}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell}, \widetilde{c}_{\mathsf{Ideal},1}, \ldots \widetilde{c}_{\mathsf{Ideal},y})\big)$$

   *over the randomness of sampling $r_1, \ldots, r_\ell$ and $r_{\mathsf{Ideal},1}, \ldots, r_{\mathsf{Ideal},\ell}$.*

In what follows, we define a slight strengthening of $\ell$-to-$y$ same-tag non-malleability w.r.t. replacement. Namely, in the definition below we allow the MIM to *obtain as input* some restricted auxiliary information on the honest messages and randomness.

**Definition 3 ($\ell$-to-$y$ Same-tag Auxiliary-Input Non-malleable Commitments w.r.t. Replacement).** *A non-interactive non-malleable commitment scheme with $N$ tags consists of a probabilistic poly-time algorithm $\mathcal{C}$, that takes as input a message $m \in \{0,1\}^p$, randomness $r \in \{0,1\}^{\mathsf{poly}(n)}$, and a $\mathsf{tag} \in [N]$, and outputs a commitment $\mathsf{com}_{\mathsf{tag}}(m;r)$. It is said to be $\ell$-to-$y$ same-tag auxiliary-input non-malleable w.r.t. replacement for polynomials $\ell(\cdot)$ and $y(\cdot)$, if the following two properties hold:*

1. **Statistical binding.** *There do not exist* $m_0, m_1 \in \{0,1\}^p$, $r_0, r_1 \in \{0,1\}^{\mathsf{poly}(n)}$ *and* $\mathsf{tag}_0, \mathsf{tag}_1 \in [N]$ *such that* $m_0 \neq m_1$ *and* $\mathsf{com}_{\mathsf{tag}_0}(m_0; r_0) = \mathsf{com}_{\mathsf{tag}_1}(m_1; r_1)$.

2. $\ell$**-to-**$y$ **Non-malleability.** *There exists a function* $t_V : \mathbb{N} \to \mathbb{N}$ *such that the following holds.*

   *Fix any messages* $m_1, \ldots m_\ell \in \{0,1\}^p$, *any* $\mathsf{tag}_1, \ldots \mathsf{tag}_\ell$, *and any efficient auxiliary input functions* $\mathsf{aux}_1, \mathsf{aux}_2, \ldots, \mathsf{aux}_\ell$, *where for every* $i \in [\ell]$, $\mathsf{aux}_i$ *takes as input the commitments* $(c_1, \ldots c_\ell)$ *together with the messages and randomness used to compute* $(c_1, \ldots c_{i-1}, c_{i+1}, \ldots, c_\ell)$. *Set* $T_V(n) = 2^{t_V(n)}$.

   *For every* $\beta \in [\ell]$ *define* $\ell$ *commitments* $c_{\beta,1}, \ldots, c_{\beta,\ell}$, *where* $c_{\beta,i} = \mathsf{com}_{\mathsf{tag}_i}(0^p; r_i)$ *for every* $i \in [\beta]$, *and* $c_{\beta,i} = \mathsf{com}_{\mathsf{tag}_i}(m_i; r_i)$ *for every* $i \in [\beta+1, \ell]$, *where* $r_1, \ldots, r_\ell \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$.

   *Suppose that for every* $\beta \in [0, \ell-1]$,

$$\left(c_{\beta,1}, \ldots, c_{\beta,\ell}, \mathsf{aux}_\beta(c_{\beta,1}, \ldots, c_{\beta,\ell}, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots, r_{\beta-1}, r_{\beta+1}, \ldots, r_\ell)\right) \approx_{T_V(n)} \tag{1}$$

$$(c_{\beta,1}, \ldots, c_{\beta,\ell}, \mathsf{aux}_{\beta+1}(c_{\beta,1}, \ldots, c_{\beta,\ell}, (0^p)_{\times(\beta)}, m_{\beta+2}, \ldots, m_\ell, r_1, \ldots, r_\beta, r_{\beta+2}, \ldots, r_\ell))$$

   *where* $\mathsf{aux}_0 \triangleq \mathsf{aux}_\ell$.

   *Fix any polynomial-size adversary* $\mathcal{A}$, *and for every* $\beta \in [0, \ell]$ *let*

$$(\widetilde{c}_{\beta,1}, \ldots, \widetilde{c}_{\beta,y}, z_\beta) = \mathcal{A}(c_{\beta,1}, \ldots, c_{\beta,\ell}, \mathsf{aux}_\beta(c_{\beta,1}, \ldots c_{\beta,\ell}, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots, r_{\beta-1}, r_{\beta+1}, \ldots, r_\ell)).$$

   *We require that there exist (possibly inefficient) functions* $\mathcal{V}_{\mathsf{Real}}$ *and* $\mathcal{V}_{\mathsf{Ideal}}$, *each computable in time* $T_V(n)$, *such that:*

   (a) *If there exists* $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i\in[\ell]}$ *such that* $\widetilde{c}_{0,1}, \ldots \widetilde{c}_{0,y}$ *all use tag* $\widetilde{\mathsf{tag}}$, *then continue. Otherwise set* $(\widetilde{m}_1, \ldots \widetilde{m}_n) = \mathsf{abort}$.
   *For each* $i \in [y]$, *if there exists* $\widetilde{M}_i \in \{0,1\}^p$ *and* $\widetilde{r}_i \in \{0,1\}^{\mathsf{poly}(n)}$ *for which* $\widetilde{c}_{0,i} = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_i; \widetilde{r}_i)$, *set* $\widetilde{m}_i = \widetilde{M}_i$, *and otherwise no restrictions are placed on* $\widetilde{m}_i$. *We require that*

$$\Pr[\mathcal{V}_{\mathsf{Real}}(c_{0,1}, \ldots, c_{0,\ell}, \mathsf{a}_0, \widetilde{c}_{0,1}, \ldots \widetilde{c}_{0,y}) = (\widetilde{m}_1, \ldots, \widetilde{m}_y)] = 1 - \mathsf{negl}(n)$$

   *where* $\mathsf{a}_0 = \mathsf{aux}_0(c_{0,1}, \ldots, c_{0,\ell}, m_1, \ldots, m_{\ell-1}, r_1, \ldots r_{\ell-1})$.

   (b) *If there exists* $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i\in[\ell]}$ *such that* $\widetilde{c}_{\ell,1}, \ldots \widetilde{c}_{\ell,y}$ *all use tag* $\widetilde{\mathsf{tag}}$, *then continue. Otherwise set* $(\widetilde{m}_1, \ldots \widetilde{m}_n) = \mathsf{abort}$.
   *For each* $i \in [y]$, *if there exists* $\widetilde{M}_i \in \{0,1\}^p$ *and* $\widetilde{r}_i \in \{0,1\}^{\mathsf{poly}(n)}$ *for which* $\widetilde{c}_{\ell,i} = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_i; \widetilde{r}_i)$, *set* $\widetilde{m}_i = \widetilde{M}_i$, *and otherwise no restrictions are placed on* $\widetilde{m}_i$. *We require that*

$$\Pr[\mathcal{V}_{\mathsf{Ideal}}(c_{\ell,1}, \ldots, c_{\ell,\ell}, \mathsf{a}_\ell, \widetilde{c}_{\ell,1}, \ldots, \widetilde{c}_{\ell,y}) = (\widetilde{m}_1, \ldots, \widetilde{m}_y)] = 1 - \mathsf{negl}(n)$$

   *where* $\mathsf{a}_\ell = \mathsf{aux}_\ell(c_{\ell,1}, \ldots, c_{\ell,\ell}, (0^p)_{\times(\ell-1)}, r_1, \ldots r_{\ell-1})$.

   (c) *We require:*

$$\left((c_{0,1}, \ldots c_{0,\ell}), \mathsf{a}_0, (\widetilde{c}_{0,1}, \ldots \widetilde{c}_{0,y}), z_0, \mathcal{V}_{\mathsf{Real}}(c_{0,1}, \ldots, c_{0,\ell}, \mathsf{a}_0, \widetilde{c}_{0,1}, \ldots \widetilde{c}_{0,y})\right) \approx_c$$

$$\left((c_{\ell,1}, \ldots c_{\ell,\ell}), \mathsf{a}_\ell, (\widetilde{c}_{\ell,1}, \ldots \widetilde{c}_{\ell,y}), z_\ell, \mathcal{V}_{\mathsf{Ideal}}(c_{\ell,1}, \ldots, c_{\ell,\ell}, \mathsf{a}_\ell, \widetilde{c}_{\ell,1}, \ldots \widetilde{c}_{\ell,y})\right)$$

   *over the randomness of sampling* $c_{0,1}, \ldots, c_{0,\ell}$ *and* $c_{\ell,1}, \ldots, c_{\ell,\ell}$.

**Remark 1.** *One can strengthen these definitions, to require non-malleability to hold for* any two sets of messages $(m_1^1, \ldots m_\ell^1)$ *and* $(m_1^2, \ldots, m_\ell^2)$, *such that* $\mathcal{V}_{\mathsf{Real}}$ *(as before) considers an experiment where the honest committer generates commitments to* $(m_1^1, \ldots m_\ell^1)$, *whereas* $\mathcal{V}_{\mathsf{Ideal}}$ *considers an experiment where the honest committer generates commitments to* $(m_1^2, \ldots, m_\ell^2)$ *(instead of generating commitments to* 0*s). The proofs of Theorem 1 and Theorem 2 show that our constructions also satisfy this stronger definition.*

### 3.2 Non-Malleable Commitments w.r.t. Commitment

In this section, we consider the stronger definition of non-malleability with respect to commitment [PR05b]. This definition is sometimes considered in the many-to-many setting (known as concurrent non-malleability), where the adversary (man-in-the-middle) receives many commitments "on the left" and generates many commitments "on the right". It is also sometimes considered in the one-to-one setting, where the man-in-the-middle receives a single commitment "on the left" and generates a single commitment "on the right". In what follows we present a hybrid between these two variants, where we require the MIM to use the same tag in all "right" commitments, and we refer to this as the many-to-$k$ same-tag variant. This hybrid definition is used as a stepping stone to achieve our main result.

**Definition 4** ($\ell$**-to-Many Same-tag Non-malleable Commitments with respect to Commitment).** *A non-interactive non-malleable commitment scheme with $N$ tags consists of a probabilistic poly-time algorithm $\mathcal{C}$, that takes as input a message $m \in \{0,1\}^p$, randomness $r \in \{0,1\}^{\mathsf{poly}(n)}$, and a tag $\mathsf{tag} \in [N]$, and outputs a commitment $\mathsf{com}_{\mathsf{tag}}(m;r)$. It is said to be $\ell$-to-many same-tag non-malleable with respect to commitment if the following properties hold.*

1. **Statistical binding.** *There do not exist $m_0, m_1 \in \{0,1\}^p$, $r_0, r_1 \in \{0,1\}^{\mathsf{poly}(n)}$ and $\mathsf{tag}_0, \mathsf{tag}_1 \in [N]$ such that $m_0 \neq m_1$ and $\mathsf{com}_{\mathsf{tag}_0}(m_0; r_0) = \mathsf{com}_{\mathsf{tag}_1}(m_1; r_1)$.*

2. $\ell$**-to-many Non-malleability.** *There exists a (possibly inefficient) function $\mathcal{V}$ such that the following holds:*

   - *For any $m_1, \ldots, m_\ell \in \{0,1\}^p$, any $r_1, \ldots, r_\ell \in \{0,1\}^{\mathsf{poly}(n)}$, and any $\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell \in [N]$, set $c_i = \mathsf{com}_{\mathsf{tag}_i}(m_i; r_i)$ for every $i \in [\ell]$, and let $(\widetilde{c}_1, \ldots, \widetilde{c}_k, z) = \mathcal{A}(c_1, \ldots, c_\ell)$.*
     *If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i \in [\ell]}$ such that $\widetilde{c}_1, \ldots \widetilde{c}_y$ all use $\widetilde{\mathsf{tag}}$, then continue. Otherwise set $(\widetilde{m}_1, \ldots \widetilde{m}_n) = \mathsf{abort}$.*
     *For each $i \in [k]$, if there exists $\widetilde{M}_i \in \{0,1\}^p$ and $\widetilde{r}_i \in \{0,1\}^{\mathsf{poly}(n)}$ for which $\widetilde{c}_i = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_i, \widetilde{r}_i)$, set $\widetilde{m}_i = \widetilde{M}_i$, and otherwise set $\widetilde{m}_i = \perp$.*
     *We require that $\mathcal{V}(c_1, \ldots, c_\ell, \widetilde{c}_1, \ldots, \widetilde{c}_k) = (\widetilde{m}_1, \ldots, \widetilde{m}_k)$.*
   - *For any $r_{\mathsf{Ideal},1}, \ldots, r_{\mathsf{Ideal},\ell} \in \{0,1\}^{\mathsf{poly}(n)}$, any $\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell \in [N]$, set $c_{\mathsf{Ideal},i} = \mathsf{com}_{\mathsf{tag}_i}(0^p; r_{\mathsf{Ideal},i})$ for every $i \in [\ell]$, and let $(\widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},k}, z_{\mathsf{Ideal}}) = \mathcal{A}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell})$.*
     *If there exists $\widetilde{\mathsf{tag}} \in [N] \setminus \{\mathsf{tag}_i\}_{i \in [\ell]}$ such that $\widetilde{c}_{\mathsf{Ideal},1}, \ldots \widetilde{c}_{\mathsf{Ideal},y}$ all use $\widetilde{\mathsf{tag}}$, then continue. Otherwise set $(\widetilde{m}_1, \ldots \widetilde{m}_n) = \mathsf{abort}$.*
     *For each $i \in [k]$, if there exists $\widetilde{M}_{\mathsf{Ideal},i} \in \{0,1\}^p$ and $\widetilde{r}_{\mathsf{Ideal},i} \in \{0,1\}^{\mathsf{poly}(n)}$ for which $\widetilde{c}_i = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_{\mathsf{Ideal},i}; \widetilde{r}_{\mathsf{Ideal},i})$, set $\widetilde{m}_{\mathsf{Ideal},i} = \widetilde{M}_{\mathsf{Ideal},i}$, and otherwise set $\widetilde{m}_{\mathsf{Ideal},i} = \perp$.*
     *We require that*

$$\mathcal{V}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell}, \widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},k}) = (\widetilde{m}_{\mathsf{Ideal},1}, \ldots, \widetilde{m}_{\mathsf{Ideal},k}).$$

   - *For any $m_1, \ldots, m_\ell \in \{0,1\}^p$, any $\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell \in [N]$, and for $r_1, \ldots, r_\ell \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$ and $r_{\mathsf{Ideal},1}, \ldots, r_{\mathsf{Ideal},\ell} \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$, set $c_i = \mathsf{com}_{\mathsf{tag}_i}(m_i; r_i)$ and $c_{\mathsf{Ideal},i} = \mathsf{com}_{\mathsf{tag}_i}(0^p; r_{\mathsf{Ideal},i})$ for every $i \in [\ell]$. Then,*

$$(c_1, \ldots, c_\ell, \widetilde{c}_1, \ldots, \widetilde{c}_k, z), \mathcal{V}(c_1, \ldots, c_\ell, \widetilde{c}_1, \ldots, \widetilde{c}_k) \approx_c$$

$$(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell}, \widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},k}, z_{\mathsf{Ideal}}), \mathcal{V}(c_{\mathsf{Ideal},1}, \ldots, c_{\mathsf{Ideal},\ell}, \widetilde{c}_{\mathsf{Ideal},1}, \ldots, \widetilde{c}_{\mathsf{Ideal},k}).$$

A hybrid argument from Lin *et. al* [LPV] shows that Definition 4 above is equivalent to the seemingly weaker definition of 1-to-many same-tag non-malleability, and the seemingly stronger definition of many-to-many same-tag non-malleability, both defined below.

**Definition 5** (**1-to-many Same-tag Non-malleable Commitments with respect to Commitment).** *We say that a commitment scheme is 1-to-many same-tag non-malleable with respect to commitment if the scheme satisfies Definition 4 for $\ell(n) = 1$.*

**Definition 6** (**Many-to-many Same-tag Non-malleable Commitments with respect to Commitment).** *We say that a commitment scheme is many-to-many same-tag non-malleable with respect to commitment if for every polynomial $\ell(\cdot)$, it is $\ell$-to-many same-tag non-malleable w.r.t. commitment (as in Definition 4).*

**Remark 2.** *We note that Definition 6 is strictly stronger than Definition 3. Any $\ell$-to-many same-tag non-malleable commitment w.r.t. commitment* com *is also an $\ell$-to-many same-tag auxiliary-input non-malleable commitment w.r.t. replacement for any polynomial $\ell$.*

*This follows by setting $t_V(n) = p + \mathsf{poly}(n)$, i.e., the time required to brute-force break the commitment, such that $\mathcal{V}$ is computable in time at most $\mathsf{poly}\big(2^{t_V(n)}\big)$,. We can then carrying out a hybrid argument (due to Lin et al. [LPV]). In the $i^{th}$ hybrid for $i \in [y]$, $(c_1, \ldots c_i)$ are generated as commitments to $0^p$, and $(c_{i+1}, \ldots c_y)$ are generated as commitments to $(m_{i+1}, \ldots, m_y)$; as defined, $\mathsf{aux}_i$ is generated as a function of all but the randomness used to generate the $i^{th}$ commitment. Indistinguishability between $\mathsf{Hybrid}_i$ and $\mathsf{Hybrid}_{i+1}$ follows by non-malleability w.r.t. commitment of* com *applied to $c_i$, and by the $T_V(n)$-indistinguishability of $(\mathsf{aux}_i, \mathsf{aux}_{i+1})$.*

# 4 Non-Malleable Commitments for Small Tags

In this section, we construct a many-to-many same-tag non-malleable commitment scheme with respect to commitment (Definition 6) for $\eta \cdot \log\log(n)$ tags, for a small constant $\eta > 0$. This scheme can be used to instantiate our compiler from Section 5 (see Section 6 for details).

## 4.1 Non-Malleable Commitment Scheme for $\eta \cdot \log\log n$ Tags

In this section, we construct a many-to-many same-tag non-malleable commitment scheme w.r.t. commitment (Definition 6) for $\zeta = \eta \cdot \log\log n$ tags, for a small enough constant $\eta > 0$, based on the following assumption about non-interactive bit commitments.

**Assumption 1.** *There exist non-interactive bit commitments $\mathsf{com}_0 : \{0,1\} \times \{0,1\}^n \to \{0,1\}^{L(n)}$ and $\mathsf{com}_1 : \{0,1\} \times \{0,1\}^n \to \{0,1\}^{L(n)}$ with the following properties.*

1. **There exists an oracle relative to which $\mathsf{com}_0$ is *sub-exponentially* hiding, but $\mathsf{com}_1$ is extractable.** *There exists an (inefficient, possibly randomized) oracle $\mathcal{O}_1$ and a poly-size algorithm $\mathcal{A}_1$ such that for every $n \in \mathbb{N}$ and every $(m, r) \in \{0,1\} \times \{0,1\}^n$,*

$$\Pr[{\mathcal{A}_1}^{\mathcal{O}_1}(\mathsf{com}_1(m; r)) = (m, r)] = 1 - \mathsf{negl}(n).$$

*where the probability is over the randomness of $\mathcal{O}_1$. Moreover, on input any string $c$ for which $\nexists (m, r)$ such that $c = \mathsf{com}_1(m; r)$, we require that $\mathcal{A}_1^{\mathcal{O}_1}$ output $\perp$.*

*Yet, there exists a constant $\delta > 0$ such that for every $n \in \mathbb{N}$, every $\mathsf{poly}\left(2^{n^\delta}\right)$-size adversary $\mathcal{A}$, and every pair of messages $m_1$ and $m_2$ in $\{0,1\}$,*

$$\left|\Pr[\mathcal{A}^{\mathcal{O}_1}(\mathsf{com}_0(m_1;r))=1] - \Pr[\mathcal{A}^{\mathcal{O}_1}(\mathsf{com}_0(m_2;r))=1]\right| = \mathsf{negl}(n),$$

*where the probability is over $r \xleftarrow{\$} \{0,1\}^n$ and over the randomness of $\mathcal{O}_1$.*

2. **There exists an oracle relative to which $\mathsf{com}_1$ is *sub-exponentially* hard to invert but $\mathsf{com}_0$ is invertible.** *There exists an (inefficient, possibly randomized) oracle $\mathcal{O}_0$ and a poly-size algorithm $\mathcal{A}_0$ such that for every $n \in \mathbb{N}$ and every $(m,r) \in \{0,1\} \times \{0,1\}^n$,*

$$\Pr[\mathcal{A}_0^{\mathcal{O}_0}(\mathsf{com}_0(m;r)) = (m,r)] = 1 - \mathsf{negl}(n)$$

*where the probability is over the randomness of $\mathcal{O}_0$. Moreover, on input any string $c$ for which $\nexists (m,r)$ such that $c = \mathsf{com}_0(m;r)$, we require that $\mathcal{A}_0^{\mathcal{O}_0}$ output $\perp$.*

*Yet, there exists a constant $\delta > 0$ such that for every $n \in \mathbb{N}$, every $\mathsf{poly}\left(2^{n^\delta}\right)$-size adversary $\mathcal{A}$, and every pair of messages $m_1$ and $m_2$ in $\{0,1\}$,*

$$\left|\Pr[\mathcal{A}^{\mathcal{O}_0}(\mathsf{com}_1(m_1;r))=1] - \Pr[\mathcal{A}^{\mathcal{O}_0}(\mathsf{com}_1(m_2;r))=1]\right| = \mathsf{negl}(n),$$

*where the probability is over $r \xleftarrow{\$} \{0,1\}^n$ and over the randomness of $\mathcal{O}_0$.*

In Section 4.2, we describe how to instantiate this assumption based on specific cryptographic assumptions. Pass and Wee [PW10] showed that Assumption 1 can be used to derive a sequence of commitments, described below.

There exist inefficient (possibly randomized) oracles $\mathcal{O}_0, \mathcal{O}_1$, a small constant $\eta > 0$, and a sequence $\{\mathsf{com}_{b,i}\}_{b\in\{0,1\},i\in[\zeta]}$ of commitment functions, where $\zeta = \eta \cdot \log\log(n)$ and

$$\mathsf{com}_{b,i} : \{0,1\} \times \{0,1\}^{\ell_{b,i}(n)} \to \{0,1\}^{L(\ell_{b,i}(n))}$$

such that for each $b \in \{0,1\}$,

$$\ell_{b,1} = \omega(\log n^{\log\log n}) < \ell_{b,2} < \ldots < \ell_{b,\zeta-1} < \ell_{b,\zeta} \triangleq n$$

and for every $i,j,k \in [\zeta]$ such that $k > i$, inverting $\mathsf{com}_{b,k}$ relative to the oracle $\mathcal{O}_{1-b}$ requires more time than jointly inverting $\mathsf{com}_{b,i}$ and $\mathsf{com}_{1-b,j}$ relative to the oracle $\mathcal{O}_{1-b}$.

Formally, for every $b \in \{0,1\}$ and every $i \in [\zeta-1]$ there exists a $T_{b,i} \cdot \mathsf{poly}(n)$-size algorithm $\mathcal{A}_{b,i}$ such that for every $j \in [\zeta]$, every messages $m_1, m_2 \in \{0,1\}$, every $r \in \{0,1\}^{\ell_{b,i}}$ and $r' \in \{0,1\}^{\ell_{1-b,j}}$,

$$\Pr\left[\left(\mathcal{A}_{b,i}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,i}(m_1;r)) = (m_1,r)\right) \ \wedge \ \left(\mathcal{A}_{b,i}^{\mathcal{O}_{1-b}}(\mathsf{com}_{1-b,j}(m_2;r')) = (m_2,r')\right)\right] = 1 - \mathsf{negl}(n),$$

where the probability is over the randomness of $\mathcal{O}_{1-b}$. Moreover, on input any element outside the range of $\mathsf{com}_{b,i}$ or $\mathsf{com}_{1-b,j}$, $\mathcal{A}_{b,i}^{\mathcal{O}_{1-b}}$ outputs $\perp$.

Yet, for every $\mathsf{poly}(T_{b,i})$-size adversary $\mathcal{A}$ and every $k > i$,

$$\left|\Pr[\mathcal{A}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,k}(m_1;r))=1] - \Pr[\mathcal{A}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,k}(m_2;r))=1]\right| = \mathsf{negl}(n),$$

where the probability is over $r \leftarrow \{0,1\}^{\ell_{b,k}(n)}$ and over the randomness of $\mathcal{O}_{1-b}$.

**Overview of the construction of the commitment sequence.** This is only for completeness and is taken from Pass and Wee [PW10]. This sequence of commitments is constructed as follows. For every $b \in \{0,1\}$ and every $i \in [0, \zeta - 1]$, set $\ell_{b,i+1} = \ell_{b,i}^{1/\delta}$ (where $\delta \in (0,1)$ is the constant from Assumption 1). Note that if $\eta < \frac{1}{\log 1/\delta}$ then setting $\delta' \triangleq \eta \cdot \log(1/\delta) < 1$, the following holds

$$\ell_{b,0} = (\ell_{b,\zeta})^{\delta^\zeta} = (\ell_{b,\zeta})^{(1/\log n)^{\delta'}} = n^{(1/\log n)^{\delta'}} = 2^{\log n^{(1-\delta')}}.$$

For every $i \in [\zeta]$ and $b \in \{0,1\}$, the commitment $\mathsf{com}_{b,i} : \{0,1\} \times \{0,1\}^{\ell_{b,i}(n)} \to \{0,1\}^{L(\ell_{b,i}(n))}$ is defined by

$$\mathsf{com}_{b,i}(m; r) = \mathsf{com}_b(m; r) \text{ where } \mathsf{com}_b \text{ is invoked with security parameter } \ell_{b,i}(n).$$

**Remark 3.** *In what follows we think of* $\mathsf{com}_b : \{0,1\} \times \{0,1\}^* \to \{0,1\}^*$*, where inputs of length* $n$ *are mapped to inputs of length* $L(n)$*.*

For every $b \in \{0,1\}$ and every $i \in [\zeta - 1]$, setting $T_{b,i} = 2^{\ell_{b,i}}$,

$$T_{b,i+1} = 2^{\ell_{b,i+1}} = 2^{\ell_{b,i}^{1/\delta}} = T_{b,i}^{\omega(1)},$$

as desired, where the latter equality follows from the fact that $\delta$ is a constant smaller than 1.

For every $b \in \{0,1\}$ and every $i \in [\zeta]$, consider the algorithm $\mathcal{A}_{b,i}$ that inverts $\mathsf{com}_{b,i}$ by enumerating over all possible $r \in \{0,1\}^{\ell_{b,i}}$, and outputs $\perp$ if no such $r$ is found. Clearly, $\mathcal{A}_{b,i}$ runs in time at most $T_{b,i} \cdot \mathsf{poly}(n)$. Moreover, for any $j \in [\zeta]$ and any $r' \in \{0,1\}^{\ell_{1-b,j}}$, the algorithm $\mathcal{A}_{b,i}$, on input $\mathsf{com}_{1-b,j}(r')$ and given oracle access to $\mathcal{O}_{1-b}$, runs in poly-time and outputs $\mathcal{A}_{1-b}^{\mathcal{O}_{1-b}}(f_{1-b,j}(r'))$. Thus, for every $b \in \{0,1\}$ and every $i \in [\zeta - 1]$, $\mathcal{A}_{b,i}$ is a $T_{b,i} \cdot \mathsf{poly}(n)$-size algorithm such that for every $j \in [\zeta]$, every $m_1, m_2 \in \{0,1\}$, every $r \in \{0,1\}^{\ell_{b,i}}$ and every $r' \in \{0,1\}^{\ell_{1-b,j}}$,

$$\Pr\Big[\big(\mathcal{A}_{b,i}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,i}(m_1; r)) = (m_1, r)\big) \ \wedge \ \big(\mathcal{A}_{b,i}^{\mathcal{O}_{1-b}}(\mathsf{com}_{1-b,j}(m_2; r')) = (m_2, r')\big)\Big] = 1 - \mathsf{negl}(n),$$

where the probability is over the randomness of $\mathcal{O}_{1-b}$, as desired.

By sub-exponential hardness of $\mathsf{com}_b$ in the presence of $\mathcal{O}_{1-b}$ (which is implied by Assumption 1), it follows that for $k \geq (i+1)$, inverting $\mathsf{com}_{b,k}$ given oracle to $\mathcal{O}_{1-b}$ requires circuits of size greater than $\mathsf{poly}\left(2^{\ell_{b,i+1}^{\delta}}\right) = \mathsf{poly}\left(2^{\ell_{b,i}}\right) = \mathsf{poly}\left(T_{b,i}\right)$. Therefore, for any $\mathsf{poly}(T_{b,i})$-size adversary $\mathcal{A}$ and every $k > i$,

$$\Big|\Pr[\mathcal{A}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,k}(m_1; r)) = 1] - \Pr[\mathcal{A}^{\mathcal{O}_{1-b}}(\mathsf{com}_{b,k}(m_2; r)) = 1]\Big| = \mathsf{negl}(n),$$

where the probability is over $r \xleftarrow{\$} \{0,1\}^{\ell_{b,k}(n)}$ and over the randomness of $\mathcal{O}_{1-b}$, as desired. The fact that $\ell_{b,0} \geq 2^{\log n^{(1-\delta')}}$ (for some constant $\delta' < 1$), implies that for $i \in [\zeta]$,

$$T_{b,i} \triangleq 2^{\ell_{b,i}} \geq 2^{\log^c n},$$

for every constant $c \in \mathbb{N}$.

**Our construction of non-malleable commitments for $\zeta(n)$ tags** To commit to a message $m = (m_1, \ldots, m_p) \in \{0,1\}$ with respect to tag, using randomness $(r_i, s_i, a_i)_{i\in[p]}$, where for every $i \in [p]$, $r_i, s_i \xleftarrow{\$} \{0,1\}^{\ell_{0,\mathsf{tag}}} \times \{0,1\}^{\ell_{1,\zeta-\mathsf{tag}}}$ and $a_i \xleftarrow{\$} \{0,1\}$, our commitment algorithm is defined by:

$$\begin{aligned}&\mathsf{Com}_{\mathsf{tag}}\Big(m; (r_i, s_i, a_i)_{i\in[p]}\Big)\\ &= \Big(\mathsf{tag}, \big(\mathsf{com}_{0,\mathsf{tag}}(a_i; r_i)\big)_{i\in[p]}, \big(\mathsf{com}_{1,\zeta-\mathsf{tag}}(m_i \oplus a_i; s_i)\big)_{i\in[p]}\Big).\end{aligned}$$

**Theorem 1.** *If Assumption 1 holds, then there exists a constant $\eta > 0$ such that $\mathsf{Com}_{\mathsf{tag}}$ is a non-interactive many-to-many same-tag non-malleable commitment scheme w.r.t. commitment (Definition 6) for $\zeta = \eta \cdot \log\log(n)$ tags, against all $2^{\mathsf{poly}(\log n)}$-size adversaries.*

*Proof.* The fact that Com is statistically binding follows from the fact that $\mathsf{com}_{b,i}$ are all statistically binding, which in turn follows from the fact that $\mathsf{com}_0$ and $\mathsf{com}_1$ are statistically binding. We next argue that Com is many-to-many same-tag non-malleable w.r.t. commitment (Definition 6), against all $2^{\mathsf{poly}(\log n)}$-size adversaries. To this end, it suffices to prove that it is 1-to-many same-tag non-malleable w.r.t. commitment (Definition 5), against all $2^{\mathsf{poly}(\log n)}$-size adversaries. This follows by a hybrid argument of [LPV], which proves that any commitment scheme that satisfies Definition 5 also satisfies Definition 6 (and this hybrid argument also holds for $2^{\mathsf{poly}(\log n)}$-size adversaries).

To prove non-malleability, fix a $2^{\mathsf{poly}(\log n)}$-size adversary $\mathcal{A}$, and fix any $k \leq \mathsf{poly}(n)$. Given a message $m = (m_1, \ldots, m_p) \in \{0,1\}^p$,[16] we consider the following distribution:

Choose at random $b \xleftarrow{\$} \{0,1\}$ and $R \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$. If $b = 0$ then let $c = \mathsf{Com}_{\mathsf{tag}}(0^p; R)$. If $b = 1$ then let $c = \mathsf{Com}_{\mathsf{tag}}(m; R)$. Let

$$(\widetilde{\mathsf{tag}}, \widetilde{c}_1, \ldots, \widetilde{c}_k) = \mathcal{A}(c).$$

Consider the joint distribution

$$(c, \widetilde{c}_1, \ldots \widetilde{c}_k, \widetilde{m}_1, \ldots \widetilde{m}_k),$$

where for every $i \in [k]$, if there exists $\widetilde{M}_i \in \{0,1\}^p$ and randomness $R_i \in \{0,1\}^{\mathsf{poly}(n)}$ such that $\widetilde{c}_i = \mathsf{com}_{\widetilde{\mathsf{tag}}}(\widetilde{M}_i, R_i)$, then $\widetilde{m}_i = \widetilde{M}_i$; else $\widetilde{m}_i = \perp$.

To prove that this construction satisfies Definition 5, it suffices to prove that for every $2^{\mathsf{poly}(\log n)}$-size adversary $\mathcal{D}$ and every message $m$,

$$\Pr[\mathcal{D}(c, \widetilde{c}_1, \ldots, \widetilde{c}_k, \widetilde{m}_1, \ldots, \widetilde{m}_k) = b] = \frac{1}{2} + \mathsf{negl}(n).$$

To prove this, it suffices to show that for every $2^{\mathsf{poly}(\log n)}$-size adversary $\mathcal{D}$ and every message $m$, if $\Pr[\widetilde{\mathsf{tag}} > \mathsf{tag}] \geq \frac{1}{\mathsf{poly}(n)}$ for some polynomial $\mathsf{poly}(\cdot)$, then

$$\Pr[\mathcal{D}(c, \widetilde{c}_1, \ldots, \widetilde{c}_k, \widetilde{m}_1, \ldots, \widetilde{m}_k) = b | \widetilde{\mathsf{tag}} > \mathsf{tag}] = \frac{1}{2} + \mathsf{negl}(n),$$

and if $\Pr[\widetilde{\mathsf{tag}} < \mathsf{tag}] \geq \frac{1}{\mathsf{poly}(n)}$ for some polynomial $\mathsf{poly}(\cdot)$, then

$$\Pr[\mathcal{D}(c, \widetilde{c}_1, \ldots, \widetilde{c}_k, \widetilde{m}_1, \ldots, \widetilde{m}_k) = b | \widetilde{\mathsf{tag}} < \mathsf{tag}] = \frac{1}{2} + \mathsf{negl}(n).$$

[16] We overload notation, here $m_i$ denotes the $i^{th}$ bit of $m$, and below each $\widetilde{m}_i$ consists of $p$ bits.

Suppose that $\Pr[\widetilde{\mathsf{tag}} > \mathsf{tag}] = \widehat{p} = \frac{1}{\mathsf{poly}(n)}$. Note that $\widetilde{\mathsf{tag}} > \mathsf{tag}$ implies, $\zeta - \widetilde{\mathsf{tag}} < \zeta - \mathsf{tag}$.

Suppose for the sake of contradiction that there exists a $2^{\mathsf{poly}(\log n)}$-size distinguisher $\mathcal{D}$ and a non-negligible function $\Delta$ such that

$$\Pr[\mathcal{D}(c, \widetilde{c}_1, \ldots, \widetilde{c}_k, \widetilde{m}_1, \ldots, \widetilde{m}_k) = b | \widetilde{\mathsf{tag}} > \mathsf{tag}] \geq \frac{1}{2} + \Delta. \tag{2}$$

Consider the following hybrid distributions $H_0, \ldots, H_p$, where $H_\alpha$ is defined by choosing $m' = (m_1, \ldots, m_\alpha, 0, \ldots 0) \in \{0,1\}^p$ and setting $c = \mathsf{Com}_{\mathsf{tag}}(m'; r)$ for a randomly chosen $r \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$.

By a standard hybrid argument, we conclude that there exists $\alpha \in \{0, 1 \ldots, p\}$ and a $2^{\mathsf{poly}(\log n)}$-size distinguisher $\mathcal{D}'$ such that

$$\Pr[\mathcal{D}'(c, \widetilde{c}_1, \ldots \widetilde{c}_k, \widetilde{m}_1, \ldots \widetilde{m}_k | \widetilde{\mathsf{tag}} > \mathsf{tag}, H_\alpha) = 0] - \Pr[\mathcal{D}'(c, \widetilde{c}_1, \ldots \widetilde{c}_k, \widetilde{m}_1, \ldots \widetilde{m}_k | \widetilde{\mathsf{tag}} > \mathsf{tag}, H_{\alpha+1}) = 0] \geq \frac{\Delta}{p+1}. \tag{3}$$

Note that this implies that $\widetilde{m}_{\alpha+1} = 1$, since otherwise $H_\alpha$ and $H_{\alpha+1}$ are identical.

We use $\mathcal{D}$ to construct a $\mathsf{poly}(T_{1,\xi-\widetilde{\mathsf{tag}}})$-size adversary $\mathcal{B}^{\mathcal{O}_0}$ that breaks the hiding property of $\mathsf{com}_{1,\zeta-\mathsf{tag}}$, contradicting the security property of $\mathsf{com}_{1,\zeta-\mathsf{tag}}$. Recall that

$$\begin{aligned}&\mathsf{Com}_{\mathsf{tag}}\Big(m; (r_i, s_i, a_i)_{i\in[p]}\Big)\\ &= \Big(\mathsf{tag}, \big(\mathsf{com}_{0,\mathsf{tag}}(a_i; r_i)\big)_{i\in[p]}, \big(\mathsf{com}_{1,\zeta-\mathsf{tag}}(m_i \oplus a_i; s_i)\big)_{i\in[p]}\Big).\end{aligned}$$

Fix any $\mathsf{tag} \in [\zeta]$. The algorithm $\mathcal{B}^{\mathcal{O}_0}$, given input a string $C$ in the range of $\mathsf{com}_{1,\zeta-\mathsf{tag}}$, and oracle access to $\mathcal{D}$ does the following:

1. For each $j \in [p]$ sample $r_j \xleftarrow{\$} \{0,1\}^{\ell_{0,\mathsf{tag}}}$ and compute $y_j = \mathsf{com}_{0,\mathsf{tag}}(a_j; r_j)$.
2. For each $j \in [\alpha] \cup [\alpha+2, p]$, sample $s_j \xleftarrow{\$} \{0,1\}^{\ell_{1,\zeta-\mathsf{tag}}}$ and compute $w_j = \mathsf{com}_{1,\zeta-\mathsf{tag}}(m_j \oplus a_j; s_j)$.
3. Let $w_{\alpha+1} = C$.
4. Let $c = (\mathsf{tag}, \{y_j\}_{j\in[p]}, \{w_j\}_{j\in[p]})$.
5. Obtain $(\widetilde{\mathsf{tag}}, \widetilde{c}_1, \ldots, \widetilde{c}_k) = \mathcal{A}(c)$.
6. If $\widetilde{\mathsf{tag}} < \mathsf{tag}$, then output a randomly chosen $b \xleftarrow{\$} \{0,1\}$.
7. For each $\kappa \in [k]$, do the following:
   - Parse $\widetilde{c}_\kappa = (\widetilde{\mathsf{tag}}, \{\widetilde{y}_j^\kappa\}_{j\in[p]}, \{\widetilde{w}_j^\kappa\}_{j\in[p]})$.
   - For each $j \in [p]$, compute $(\widetilde{a}_j^\kappa, \widetilde{r}_j^\kappa) = \mathcal{A}^{\mathcal{O}_0}_{1,\zeta-\widetilde{\mathsf{tag}}}(\widetilde{y}_j^\kappa)$ and $(\widetilde{a'}_j^\kappa, \widetilde{s}_j^\kappa) = \mathcal{A}^{\mathcal{O}_0}_{1,\zeta-\widetilde{\mathsf{tag}}}(\widetilde{w}_j^\kappa)$.
   - If there exists $j \in [p]$ such that $a_j^\kappa = \perp$ or $a'^\kappa_j = \perp$, then set $m_\kappa = \perp$.
   - Else, set $m_\kappa = (m_1^\kappa, m_2^\kappa, \ldots m_p^\kappa)$, where $m_j^\kappa = a_j^\kappa \oplus a'^\kappa_j$.

   Recall that for every $\widetilde{\mathsf{tag}} \in [\zeta]$, $\mathcal{A}^{\mathcal{O}_0}_{1,\zeta-\widetilde{\mathsf{tag}}}$ is a $T_{1,\zeta-\widetilde{\mathsf{tag}}} \cdot \mathsf{poly}(n)$-size oracle-aided algorithm that:
   - Inverts $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$ on *any* element in the image of $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$ with overwhelming probability (over the randomness of $\mathcal{O}_0$), and outputs $\perp$ on input any element outside the image of $\mathsf{com}_{0,\widetilde{\mathsf{tag}}}$.

- Inverts $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$ on *any* element in the image of $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$ with overwhelming probability (over the randomness of $\mathcal{O}_0$), and outputs $\perp$ on input any element outside the image of $\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}$.

Therefore, $(\widetilde{m}_1, \ldots \widetilde{m}_k)$ are all extracted correctly with overwhelming probability.

8. Compute $e = \mathcal{D}'(c, \widetilde{c}_1, \ldots, \widetilde{c}_k, \widetilde{m}_1, \ldots, \widetilde{m}_k)$.
9. If $e = 0$, output $b' = a_{\alpha+1}$.
10. If $e = 1$, sample and output a uniformly random bit $b'$.

By Equation (3), together with the fact that $\widetilde{m}_1, \ldots, \widetilde{m}_k$ were computed correctly with overwhelming probability,

$$\begin{aligned}&\Pr[e = 0 | (\widetilde{\mathsf{tag}} > \mathsf{tag}) \ \wedge \ (a_{\alpha+1} \oplus b = 0)] - \\ &\Pr[e = 0 | (\widetilde{\mathsf{tag}} > \mathsf{tag}) \ \wedge \ (a_{\alpha+1} \oplus b = 1)] \geq \frac{\Delta}{p+1}.\end{aligned}$$

Since $a_{\alpha+1} \xleftarrow{\$} \{0,1\}$ (independently of $b$), this implies that

$$\begin{aligned}&\Pr[(a_{\alpha+1} \oplus b = 0) \ \wedge \ (e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] - \\ &\Pr[(a_{\alpha+1} \oplus b = 1) \ \wedge \ (e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] \geq \frac{\Delta}{2(p+1)}.\end{aligned}$$

which in turn implies that

$$\begin{aligned}&\Pr[(b' = b) \ \wedge \ (e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] - \\ &\Pr[(b' \neq b) \ \wedge \ (e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] \geq \frac{\Delta}{2(p+1)}.\end{aligned}$$

which implies

$$\Pr[(b' = b) \ \wedge \ (e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] = \frac{1}{2}\Pr[(e = 0) | \widetilde{\mathsf{tag}} > \mathsf{tag}] + \frac{\Delta}{4(p+1)}$$

Also note that we sample $b'$ uniformly at random if $e = 1$. Therefore,

$$\begin{aligned}&\Pr[(b' = b) \ \wedge \ (e = 1) | \widetilde{\mathsf{tag}} > \mathsf{tag}] - \\ &\Pr[(b' \neq b) \ \wedge \ (e = 1) | \widetilde{\mathsf{tag}} > \mathsf{tag}] = 0\end{aligned}$$

which implies

$$\Pr[(b' = b) \ \wedge \ (e = 1) | \widetilde{\mathsf{tag}} > \mathsf{tag}] = \frac{1}{2}\Pr[(e = 1) | \widetilde{\mathsf{tag}} > \mathsf{tag}]$$

This implies that

$$\Pr[\mathcal{B}^{\mathcal{O}_0}(\mathsf{com}_{1,\zeta-\widetilde{\mathsf{tag}}}(b)) = b | \widetilde{\mathsf{tag}} > \mathsf{tag}] \geq \frac{1}{2} + \frac{\Delta}{4(p+1)} - \mathsf{negl}(n),$$

contradicting Assumption 1.

The case where $\Pr[\widetilde{\mathsf{tag}} < \mathsf{tag}] = \frac{1}{\mathsf{poly}(n)}$, is identical to the previous case, with the roles of $\mathsf{com}_0$ and $\mathsf{com}_1$ reversed, thus we omit the proof.

This completes the proof of non-malleability. □

### 4.2 Instantiating the Assumption

**Claim 1.** *Assume the existence of constants $\delta > \delta' > 0$, and two families of non-interactive bit commitments $\mathcal{C}_0 : \{0,1\} \times \{0,1\}^n \to \{0,1\}^*$ and $\mathcal{C}_1 : \{0,1\} \times \{0,1\}^{n^\delta} \to \{0,1\}^*$, so that:*

- *For every $2^{n^{2\delta}}$-size adversary $\mathcal{A}$,*

$$|\Pr[\mathcal{A}(\mathcal{C}_0(0;r)) = 0] - \Pr[\mathcal{A}(\mathcal{C}_0(1;r)) = 0]| = \mathsf{negl}(n)$$

  *over the randomness of sampling $r \xleftarrow{\$} \{0,1\}^n$.*

- *There exists a polynomial-size algorithm $\mathcal{A}_0$ such that for every string $c$, $\mathcal{A}_0^{\mathsf{BQP}}(c)$ outputs $(b,r) \in \{0,1\}^{n+1}$, such that*

$$\Pr[\big(c = \mathcal{C}_0(b,r)\big) \vee \big(\ \nexists (b',r') \text{ such that } c = \mathcal{C}_0(b';r')\big)] = 1 - \mathsf{negl}(n)$$

- *For every $2^{n^{\delta'}}$-size adversary $\mathcal{A}$,*

$$|\Pr[\mathcal{A}^{\mathsf{BQP}}(\mathcal{C}_1(0;r)) = 0] - \Pr[\mathcal{A}^{\mathsf{BQP}}(\mathcal{C}_1(1;r)) = 0]| = \mathsf{negl}(n)$$

  *over the randomness of sampling $r \xleftarrow{\$} \{0,1\}^{n^\delta}$.*

*Then Assumption 1 follows by defining*

$$\mathsf{com}_0(b; r_1, r_2, \ldots r_n) \triangleq \mathcal{C}_0(b; r_1, r_2, \ldots r_n),$$

*and*

$$\mathsf{com}_1(b; r_1, r_2, \ldots r_n) \triangleq \mathcal{C}_1(b; r_1, r_2, \ldots r_{n^\delta}),$$

*and setting $\mathcal{O}_0 = \mathsf{BQP}$ and $\mathcal{O}_1 = \mathsf{DTIME}(2^{n^\delta})$.*

Concretely, it suffices to instantiate $\mathcal{C}_0$ to be any non-interactive commitment scheme whose hiding is based on the sub-exponential hardness of any problem that is invertible given a BQP oracle; for example, subexponential hardness of Factoring of Discrete Log.

Such a commitment can be obtained from any injective one-way function $F_0 : \{0,1\}^n \to \{0,1\}^*$ for which the one-wayness of $F_0$ is based on the sub-exponential hardness of Factoring (or Discrete Log), and that $F_0$ is invertible everywhere given access to an oracle that breaks Factoring (or Discrete Log) respectively. Given such an injective one-way function, the bit commitment $\mathcal{C}_0$ can be defined as follows: On input bit $b$ and randomness $r, s \in \{0,1\}^n$, output $F_0(r), s, (\langle r, s\rangle \oplus b)$. By the Goldreich-Levin hardcore theorem, the bit $b$ is computationally hidden as long as the function $F_0$ is one-way.

$\mathcal{C}_1$ can be instantiated as any commitment where the hiding property holds against sub-exponential quantum adversaries. Such commitments were recently constructed by [GHKW17] assuming sub-exponential quantum hardness of lattice-based problems, such as the learning with errors (LWE) problem or the learning parity with noise (LPN) problem. These can also be instantiated based on any injective one-way functions with sub-exponential quantum hardness, by relying on the hardcore bit technique as described above.

Below, we describe how a simplification of the assumption above gives tag-based (many-to-many) adaptive commitments for two tags, based only on sub-exponential hardness of factoring/discrete log, and quantum polynomial hardness of LWE.

**Remark 4.** *Assume the existence of a constant $0 < \delta < 1$ and two families of bit commitments $\mathcal{C}_0 : \{0,1\} \times \{0,1\}^{n^{1/\delta}} \to \{0,1\}^*$ and $\mathcal{C}_1 : \{0,1\} \times \{0,1\}^n \to \{0,1\}^*$, such that the following is true:*

- *For every $2^n$-size adversary $\mathcal{A}$,*

$$|\Pr[\mathcal{A}(\mathcal{C}_0(0;r)) = 0] - \Pr[\mathcal{A}(\mathcal{C}_0(1;r)) = 0]| = \mathsf{negl}(n)$$

  *over the randomness of sampling $r \xleftarrow{\$} \{0,1\}^{n^{1/\delta}}$.*

- *There exists a polynomial-size algorithm $\mathcal{A}_0$ such that for every string $c$, $\mathcal{A}_0^{\mathsf{BQP}}(c) \to (b,r)$ such that*

$$\Pr[\big(c = \mathcal{C}_0(b,r)\big) \vee \big(\ \nexists b', r' \text{ such that } c = \mathcal{C}_0(b';r')\big)] = 1 - \mathsf{negl}(n)$$

- *For every poly-size adversary $\mathcal{A}$,*

$$|\Pr[\mathcal{A}^{\mathsf{BQP}}(\mathcal{C}_1(0;r)) = 0] - \Pr[\mathcal{A}^{\mathsf{BQP}}(\mathcal{C}_1(1;r)) = 0]| = \mathsf{negl}(n)$$

  *over the randomness of sampling $r \xleftarrow{\$} \{0,1\}^n$.*

*Then, a tag-based adaptive commitment scheme for two tags, against polynomial-sized adversaries, can be defined as follows: $\mathsf{com}_0 \triangleq \mathcal{C}_0$ and $\mathsf{com}_1 \triangleq \mathcal{C}_1$; $\mathcal{O}_0 = \mathsf{BQP}$ and $\mathcal{O}_1 = \mathsf{DTIME}(2^n)$.*

*By [PPV08], this implies non-interactive many-to-many non-malleable commitment for two tags. In this case, $\mathcal{C}_0$ can be instantiated as any non-interactive bit commitment whose hardness is based on the sub-exponential hardness of factoring or discrete log, and $\mathcal{C}_1$ as a non-interactive bit commitment based on quantum polynomial hardness of LWE or LPN [GHKW17].*

# 5 Non-Malleability Amplification

In this section, we present a non-interactive amplification technique to bootstrap non-malleable commitments for small tags into non-malleable commitments for large tags.

We present a compiler that converts any $5\ell t$-to-$z$ same-tag *auxiliary-input* non-malleable commitment scheme *w.r.t. replacement* (Definition 3) for tags in $[t]$ into an $\ell$-to-$y$ same-tag *auxiliary-input* non-malleable commitment scheme *w.r.t. replacement* (Definition 3) for tags in $\left[\binom{t}{t/2}\right]$, for any $y$ and any $\ell$ such that $\ell y \leq \frac{z}{10}$. We describe our compiler in Figure 2. We emphasize that the size of the resulting commitment scheme grows linearly with $\ell$.

We denote the commitment scheme for tags in $[t]$ by $\mathsf{Com}$. We require the scheme $\mathsf{Com}$ to be secure against $\mathcal{T}$-size adversaries, for $\mathcal{T} = \mathsf{poly}\big(n \cdot 2^y\big)$.

Let $T_V : \mathbb{N} \to \mathbb{N}$ denote the time bound associated with $\mathsf{Com}$ (i.e., the time required to compute $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$). Our compiler assumes the existence of a NIWI (non-interactive witness indistinguishable) proof system, where witness indistinguishability holds against $\mathsf{poly}(T_V, \mathcal{T})$-size adversaries. From now, we assume for simplicity (and without loss of generality) that $T_V \geq \mathcal{T}$.

**Theorem 2.** *For any polynomials $y, z, \ell$ and $t$, where $\ell y \leq \frac{z}{10}$, assuming $\mathsf{Com}$ is $5\ell t$-to-$z$ same-tag auxiliary-input non-malleable w.r.t. replacement (Definition 3) for tags in $[t]$ against $\mathsf{poly}\Big(n \cdot 2^y\Big)$-size adversaries, and assuming sub-exponentially secure NIWI, the scheme in Figure 2 is $\ell$-to-$y$ same-tag auxiliary-input non-malleable w.r.t. replacement (Definition 3) for tags in $\left[\binom{t}{t/2}\right]$ against polynomial size adversaries.*

**Parameters:** Set $k = 10\ell$ and let $\mathbb{T}$ denote the unordered set of all possible subsets of $[t]$ of size $t/2$.

**Language $L$:** We define the language $L = \{\{C_{\lambda,j}, s_\lambda\}_{\lambda\in[t/2],j\in[k]} : \exists J \subset [k], |J| = k-1, \exists\{M_j, r_{\lambda,j}\}_{j\in J,\lambda\in[t/2]}$ s.t. $C_{\lambda,j} = \mathsf{Com}_{s_\lambda}(M_j; r_{\lambda,j})\ \forall j \in J, \lambda \in [t/2]\}$.

**Committer Input:** Message $M \in \{0,1\}^{p(n)}$, and tag $\mathsf{tag} \in [N]$, where $N = \binom{t}{t/2}$.

**Commit Stage:** To commit to a message $M$ w.r.t. tag tag, do the following:

1. Pick the $i^{th}$ element in $\mathbb{T}$, for $i = \mathsf{tag}$. Denote this element by $\{s_1, \ldots, s_{t/2}\}$.
2. **Committer Message.** For every $\lambda \in [t/2]$ and every $j \in [k]$, sample randomness $r_{\lambda,j} \xleftarrow{\$} \{0,1\}^{\mathsf{poly}(n)}$ and compute $C_{\lambda,j} = \mathsf{Com}_{s_\lambda}(M; r_{\lambda,j})$. Use witness $J = [k] \setminus \{1\}, \{M, r_{\lambda,j}\}_{\lambda\in[t/2],j\in J}$ to compute a NIWI proof $\Pi$ for the statement:
$$\{(C_{\lambda,j}, s_\lambda)\}_{\lambda\in[t/2],j\in[k]} \in L.$$
Send to the receiver the message
$$(\mathsf{tag}, \{(C_{\lambda,j}, s_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \Pi)$$
3. **Receiver Acceptance.** The receiver accepts the commitment $(\mathsf{tag}, \{(C_{\lambda,j}, s_\lambda)\}, \Pi)$ if and only if the proof $\Pi$ is accepted by the verifier of the NIWI system and $\{s_\lambda\}_{\lambda\in[t/2]}$ is the $i^{th}$ element in $\mathbb{T}$ for $i = \mathsf{tag}$.

**Reveal Stage:** The committer sends the message $M$ and the randomness $\{r_{\lambda,j}\}_{\lambda\in[t/2],\lambda\in[k]}$ to the receiver.

**Receiver Output:** The receiver verifies that all the commitments were correctly decommitted, and accepts the decommitment $\left(M, \{r_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}\right)$ if and only if $\forall\lambda, j \in [t/2] \times [k] : C_{\lambda,j} = \mathsf{Com}_{s_\lambda}(M; r_{\lambda,j})$.

Figure 2: Round-Preserving Tag Amplification

We will later invoke the compiler presented in Figure 2 with the scheme for $\eta \cdot \log\log n$ tags, that we constructed in Section 4, to obtain a scheme for $(\log n)^\epsilon$ tags for some small constant $\epsilon > 0$. Then we will invoke this compiler again on the resulting scheme to obtain a scheme for $2\log^2 n$, and then a third (and final) time on the resulting scheme to obtain a scheme for $n^{\log n}$ tags. We refer to Section 6 for details.

*Proof.* Statistical binding of the protocol in Figure 2 follows directly from the statistical binding property of the underlying commitment scheme Com. Computational hiding follows from the hiding of the underlying commitments, and the witness indistinguishability property of $\Pi$. Since the proof of non-malleability subsumes hiding, we directly prove non-malleability below. Specifically, we prove auxiliary-input non-malleability w.r.t. replacement for $T'_V = T_V + (n \cdot 2^y)^{c\log n}$, where $T_V$ is the running time of $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ corresponding to the underlying scheme Com, and where $c \in \mathbb{N}$ is a constant that will be specified towards the end of the proof. As mentioned above, throughout the proof, we assume for simplicity that $T_V > \mathsf{poly}(n \cdot 2^y)$ for all polynomials $\mathsf{poly}(\cdot)$.

To this end, fix any poly-size adversary $\mathcal{A}$, any messages $m_1, \ldots, m_\ell \in \{0,1\}^{p(n)}$, and any

tags $\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell \in [N]$, where $N = \binom{t}{t/2}$. Let $(\mathsf{aux}_1, \ldots \mathsf{aux}_\ell)$ denote any auxiliary information functions according Definition 3. We use $\mathsf{Com}_s$ to denote the non-malleable commitment for small tags and $\mathsf{com}_{\mathsf{tag}}$ to denote the scheme from Figure 2. For every $\beta \in [0, \ell]$ we define $\tau_\beta$ as follows:

- Set $c_{\beta,\alpha} = \mathsf{com}_{\mathsf{tag}_\alpha}(0^p; r_\alpha)$ where $r_\alpha \xleftarrow{\$} \{0,1\}^*$, for every $\alpha \in [1, \beta]$.
- Set $c_{\beta,\alpha} = \mathsf{com}_{\mathsf{tag}_\alpha}(m_\alpha; r_\alpha)$ where $r_\alpha \xleftarrow{\$} \{0,1\}^*$, for every $\alpha \in [\beta+1, \ell]$.
- Set $\tau_\beta \triangleq (c_{\beta,1}, \ldots c_{\beta,\ell}, \mathsf{a}_\beta, \widetilde{c}_1, \ldots, \widetilde{c}_y, z_\beta)$ where

$$\mathsf{a}_\beta = \mathsf{aux}_\beta(c_{\beta,1}, \ldots, c_{\beta,\ell}, (0^p)_{\times[\beta-1]}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)$$

  and $(\widetilde{c}_1, \ldots \widetilde{c}_y, z_\beta) = \mathcal{A}(c_{\beta,1}, \ldots c_{\beta,\ell}, \mathsf{a}_\beta)$.

We need to prove that there exist (inefficient) functions $\mathcal{V}_{\mathsf{real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ satisfying the validity condition in Definition 3 such that

$$\Big(\tau_0, \mathcal{V}_{\mathsf{Real}}(\tau_0)\Big) \approx \Big(\tau_\ell, \mathcal{V}_{\mathsf{Ideal}}(\tau_\ell)\Big).$$

We defer the description $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ to the end of this proof. In what follows, we consider an experiment where the PPT man-in-the-middle adversary $\mathcal{A}$ receives input commitments $c_i$ for every $i \in [\ell]$, and define a function that extracts the values committed by $\mathcal{A}$.

To this end, we parse $\widetilde{\mathsf{tag}}$ output by $\mathcal{A}$ as comprising of an unordered set of small tags, denoted by $\{\widetilde{s}_1, \widetilde{s}_2, \ldots, \widetilde{s}_{t/2}\}$, and $\mathsf{tag}_i = \{s_{1,i}, s_{2,i}, \ldots, s_{t/2,i}\}$ for $i \in [\ell]$. We note that if $\widetilde{\mathsf{tag}} \notin \{\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell\}$, then for every $i \in [\ell]$ there exists at least one index $\widetilde{\lambda}_i \in [t/2]$ such that $\widetilde{s}_{\widetilde{\lambda}_i} \notin \{s_{1,i}, s_{2,i}, \ldots, s_{t/2,i}\}$.

As an intermediate step, for every $\beta \in [\ell]$, we define (inefficient) functions $\mathcal{V}_{\beta,\mathsf{real}}(\tau)$ and $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)$ as follows:

$$\mathcal{V}_{\beta,\mathsf{real}}(\tau) = (\chi_1, \ldots, \chi_y)$$

where each $\chi_i = (\widetilde{M}_i, \psi_i)$, and $\widetilde{M}_i$ is a value extracted from the commitment $\widetilde{c}_i$. We require that for each $i \in [y]$ the extracted value $\widetilde{M}_i$ is correct whenever $\widetilde{c}_i$ is a valid commitment. More specifically, $\mathcal{V}_{\beta,\mathsf{real}}(\tau)$ is defined as follows:

- Parse $\tau = (c_1, \ldots c_\ell, \mathsf{a}, \widetilde{c}_1, \ldots \widetilde{c}_y, z)$.
- Parse $c_\beta = \big(\mathsf{tag}_\beta, \{(C_{\lambda,j}, s_\lambda)\}_{\lambda \in [t/2], j \in [k]}, \Pi\big)$.
- For each $i \in [y]$, parse $\widetilde{c}_i = (\widetilde{\mathsf{tag}}, \{(\widetilde{C}^i_{\lambda,j}, \widetilde{s}_\lambda)\}_{\lambda \in [t/2], j \in [k]}, \Pi_i)$.
- For every $i \in [y]$ such that $\Pi_i$ is rejected, set $\chi_i = \mathsf{REJECT}$ (note that this step is efficient).
- For $\widetilde{\mathsf{tag}} = \{\widetilde{s}_1, \ldots, \widetilde{s}_{t/2}\}$, let $\widetilde{\lambda}_\beta$ denote the smallest index such that $\widetilde{s}_{\widetilde{\lambda}_\beta} \notin \{s_{1,\beta}, s_{2,\beta}, \ldots, s_{t/2,\beta}\}$.
- Extract $(\chi_1, \ldots \chi_y)$ from $(\widetilde{c}_1, \ldots \widetilde{c}_y)$ as follows:
  1. We define auxiliary-input functions $\{\mathsf{au}_{\lambda,j}\}_{\lambda \in [t/2], j \in [k]}$ for the underlying commitment scheme $\mathsf{Com}$, as follows:

(a) For each $j' \in [k]$ define an auxiliary input function $\mathsf{au}_{j'}$, that on input

$$\left(\{C'_{\lambda,j}, s'_\lambda\}_{\lambda\in[t/2],j\in[k]}, \{M'_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]\setminus\{j'\}}, \{r'_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]\setminus\{j'\}}\right)$$

sets

$$X = \{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda\in[t/2],j\in[k]} \text{ and } W = \left([k]\setminus\{j'\}, \{M_{\lambda,j}, r_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]\setminus\{j'\}}\right).$$

If $R_L(X, W) = 1$ then it outputs a NIWI for the statement $X \in L$[17], else it outputs $\perp$.

(b) For all $\lambda \in [t/2]$ and $j \in [k]$, set $\mathsf{au}_{\lambda,j} = \mathsf{au}_j$[18].

2. We define an adversary $\mathcal{A}'$ for the underlying commitment Com, that has $\beta, m_1, \ldots m_\ell, \mathsf{tag}_1, \ldots \mathsf{tag}_\ell$ hardwired, and on input $\left(\{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}'\right)$ does the following:
   - Sample $r_1, \ldots r_\ell \xleftarrow{\$} \{0,1\}^*$.
   - For all $i \in [\ell]\setminus\{\beta\}$, generate $c_i$ using randomness $r_i$, according to the distribution of $c_{\beta-1,i}$ defined above.
   - Set $c_\beta = \left(\mathsf{tag}_\beta, \{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}'\right)$.
   - Compute $\mathsf{a}_\beta = \mathsf{aux}_\beta(c_1, \ldots c_\ell, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)$.
   - Execute $\mathcal{A}(c_1, \ldots, c_\ell, \mathsf{a}_\beta)$ to obtain $(\widetilde{c}_1, \ldots \widetilde{c}_y, z_\beta)$.
   - Let $Z = (z_\beta, c_1, \ldots, c_{\beta-1}, c_{\beta+1}, \ldots, c_\ell, \widetilde{c}_1, \ldots, \widetilde{c}_y)$.
   - For each $i \in [y]$, parse $\widetilde{c}_i = (\widetilde{\mathsf{tag}}, \{(\widetilde{C}^i_{\lambda,j}, \widetilde{s}_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \Pi_i)$.
   - Output $\left(\{(\widetilde{C}^i_{\widetilde{\lambda}_\beta,j}, \widetilde{s}_{\widetilde{\lambda}_\beta})\}_{i\in[y],j\in[k]}, Z\right)$.
3. For all $\lambda \in [t/2]$ and $j \in [k]$, set $m_{\lambda,j} = m_\beta$.
4. For all $\lambda \in [t/2]$ and $j \in [k]$, set $s_{\lambda,j} = s'_\lambda$, where $\{s'_\lambda\}_{\lambda\in[t/2]}$ are the input tags.
5. For $\{m_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{s_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{\mathsf{au}_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}$, and $\mathcal{A}'$ defined above, there exist distributions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ corresponding to the commitment scheme Com, satisfying Definition 3, which we denote by $v_{\mathsf{Real}}$ and $v_{\mathsf{Ideal}}$.[19] Compute

$$\{X^i_{\widetilde{\lambda}_\beta,j}\}_{i\in[y],j\in[k]} = v_{\mathsf{Real}}\left(\{C_{\lambda,j}, s_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \Pi, \{(\widetilde{C}^i_{\widetilde{\lambda}_\beta,j}, \widetilde{s}_{\widetilde{\lambda}_\beta})\}_{i\in[y],j\in[k]}\right).$$

6. For each $i \in [y]$, if there exists a message $\widetilde{M}$ and subset $J \subseteq [k]$ where $|J| \geq (\frac{3k}{4} + 1 - \beta)$, such that for all $j \in J$, $X^i_{\widetilde{\lambda}_\beta,j} = \widetilde{M}$, set $\chi_i = (\widetilde{M}, |J|)$, else set $\chi_i = \perp$.

- Output $(\chi_1, \ldots \chi_y)$.

We define $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)$ identically to $\mathcal{V}_{\beta,\mathsf{real}}$, except that in Step 5, it computes

$$\{X^i_{\widetilde{\lambda}_\beta,j}\}_{i\in[y],j\in[k]} = v_{\mathsf{Ideal}}\left(\{C_{\lambda,j}, s_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \Pi, \{(\widetilde{C}^i_{\widetilde{\lambda}_\beta,j}, \widetilde{s}_{\widetilde{\lambda}_\beta})\}_{i\in[y],j\in[k]}\right).$$

We have the following observation about the efficiency of $\mathcal{V}_{\beta,\mathsf{ideal}}$ and $\mathcal{V}_{\beta,\mathsf{real}}$ for $\beta \in [\ell]$.

[17] Refer to Figure 2 for a description of the language $L$.

[18] Note that $\mathsf{au}_{\lambda,j}$ as a function gets as input additional messages and randomness, which he ignores.

[19] While Definition 3 considers a vector of messages $m_1, \ldots, m_\ell$, (respectively tags $t_1, \ldots, t_\ell$ and commitments $c_1, \ldots c_\ell$), here and in the rest of the proof, we often abuse notation and denote the $t\ell/2$ "left" messages as a $t \times \ell/2$ *matrix* of messages (and similarly for tags and commitments).

**Claim 2.** *For every $\beta \in [\ell]$, the function $\mathcal{V}_{\beta,\mathsf{ideal}}$ and the function $\mathcal{V}_{\beta,\mathsf{real}}$ are computable in time $T_V(n) + \mathsf{poly}(n)$ where $T_V(n)$ is the time required to compute $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ for* Com.

We will make use of $\mathcal{V}_{1,\mathsf{real}}$ and $\mathcal{V}_{\ell,\mathsf{ideal}}$ to define the functions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ respectively. Before describing these functions, we prove some lemmas about the distributions output by the functions $\mathcal{V}_{\beta,\mathsf{real}}, \mathcal{V}_{\beta,\mathsf{ideal}}$ described above.

**Lemma 1.** *For all $\beta \in [\ell]$,*

$$\left(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\right)$$

*where $\tau_{\beta-1}, \tau_\beta$ are defined above.*

*Proof.* Fix any $\beta \in [\ell]$. Note that $c_{\beta,\alpha} \equiv c_{\beta-1,\alpha}$ for every $\alpha \neq \beta$, and the only difference between the two distributions is the following.

- $c_{\beta-1,\beta} \xleftarrow{\$} \mathsf{com}_{\mathsf{tag}_\beta}(m_\beta)$ whereas $c_{\beta,\beta} \xleftarrow{\$} \mathsf{com}_{\mathsf{tag}_\beta}(0)$.
- $\tau_{\beta-1}$ is defined with auxiliary-input function $\mathsf{aux}_{\beta-1}$, whereas $\tau_\beta$ is defined with auxiliary-input function $\mathsf{aux}_\beta$.

We prove this lemma via two hybrid experiments. These hybrids rely on auxiliary-input non-malleability w.r.t. replacement (Definition 3) of Com for tags in $[t]$, against $\mathsf{poly}(n\cdot 2^y)$-size machines. We will also rely on the witness indistinguishability of the NIWI against $\mathsf{poly}(T_V)$-size machines.

In the following hybrids, we start with $\left(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\right)$. We then switch from using $\mathsf{aux}_{\beta-1}$ to using $\mathsf{aux}_\beta$ in $\tau_{\beta-1}$. Finally, we switch from generating the $\beta^{th}$ commitment as a commitment to $m_\beta$ to generating it as a commitment to $0^p$. We note the differences between the hybrids by underlining them.

$\mathsf{Hybrid}_0$ : This hybrid is defined as follows:

- Compute $(c_1, \ldots c_\ell) := (c_{\beta-1,1}, \ldots c_{\beta-1,\ell})$ as described above, by sampling randomness $(r_1, \ldots, r_\ell)$.
- Compute $\mathsf{a}_{\beta-1} := \mathsf{aux}_{\beta-1}(c_1, \ldots c_\ell, (0^p)_{\times(\beta-2)}, m_\beta, \ldots, m_\ell, r_1, \ldots r_{\beta-2}, r_\beta, \ldots r_\ell)$.
- Obtain $(\widetilde{c}_1, \ldots \widetilde{c}_y, z) = \mathcal{A}(c_1, \ldots c_\ell, \mathsf{a}_{\beta-1})$.
- Set $\tau_{\beta-1} = (c_1, \ldots c_\ell, \mathsf{a}_{\beta-1}, \widetilde{c}_1, \ldots, \widetilde{c}_y, z)$.
- Output $\left(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\right)$ for $\mathcal{V}_{\beta,\mathsf{real}}$ defined above.

$\mathsf{Hybrid}_1$ : This is the same as the previous hybrid, except that it uses $\mathsf{aux}_\beta$ instead of $\mathsf{aux}_{\beta-1}$. Formally, this hybrid is defined as follows:

- Compute $(c_1, \ldots c_\ell) := (c_{\beta-1,1}, \ldots c_{\beta-1,\ell})$ as described above, by sampling randomness $(r_1, \ldots, r_\ell)$.
- Compute $\mathsf{a}_\beta := \mathsf{aux}_\beta(c_1, \ldots c_\ell, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)$.
- Obtain $(\widetilde{c}_1, \ldots \widetilde{c}_y, z) = \mathcal{A}(c_1, \ldots c_\ell, \mathsf{a}_\beta)$.
- Set $\tau = (c_1, \ldots c_\ell, \mathsf{a}_\beta, \widetilde{c}_1, \ldots, \widetilde{c}_y, z)$.
- Output $\left(\tau, \mathcal{V}_{\beta,\mathsf{real}}(\tau)\right)$ for $\mathcal{V}_{\beta,\mathsf{real}}$ defined above.

Recall that in both $\mathsf{Hybrid}_0$ and $\mathsf{Hybrid}_1$, $(c_1, \ldots c_\ell)$ are generated according to the distribution $(c_{\beta-1,1}, \ldots, c_{\beta-1.\ell})$. By Equation (1) (see Definition 3)

$$(c_{\beta-1,1}, \ldots, c_{\beta-1,\ell}, \mathsf{aux}_{\beta-1}(c_{\beta-1,1}, \ldots c_{\beta-1,\ell}, m_1, \ldots, m_{\beta-2}, m_\beta, \ldots, m_\ell, r_1, \ldots r_{\beta-2}, r_\beta, \ldots r_\ell)) \approx_{\mathsf{poly}(T_V)}$$

$$(c_{\beta-1,1}, \ldots c_{\beta-1,\ell}, \mathsf{aux}_\beta(c_{\beta-1,1}, \ldots c_{\beta-1,\ell}, m_1, \ldots, m_{\beta-1}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)).$$

This, together with the fact that $\mathcal{A}$ runs in polynomial time and $V_{\beta,\mathsf{real}}(\tau)$ can be computed in time $T_V + \mathsf{poly}(n)$, implies that

$$\mathsf{Hybrid}_0 \approx_{\mathsf{poly}(T_V)} \mathsf{Hybrid}_1.$$

$\mathsf{Hybrid}_2$ : This is the same as the previous hybrid, except that it computes $c_\beta$ as a commitment to $0$ (instead of a commitment to $m_\beta$). It uses $\mathcal{V}_{\beta,\mathsf{ideal}}$ instead of $\mathcal{V}_{\beta,\mathsf{real}}$ to compute $\chi_1, \ldots \chi_y$. Formally, this hybrid is defined as follows:

- Compute $(c_1, \ldots c_\ell) := \underline{(c_{\beta,1}, \ldots c_{\beta,\ell})}$ as described above, by sampling randomness $(r_1, \ldots, r_\ell)$.
- Compute $\mathsf{a}_\beta := \mathsf{aux}_\beta(c_1, \ldots c_\ell, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots, m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)$.
- Obtain $(\widetilde{c}_1, \ldots \widetilde{c}_y, z) = \mathcal{A}(c_1, \ldots c_\ell, \mathsf{a}_\beta)$.
- Set $\tau_\beta = (c_1, \ldots c_\ell, \mathsf{a}_\beta, \widetilde{c}_1, \ldots, \widetilde{c}_y, z)$.
- Output $\underline{\left(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\right)}$ for $\mathcal{V}_{\beta,\mathsf{ideal}}$ defined above.

Note that $c_1, \ldots c_{\beta-1}, c_{\beta+1}, \ldots c_\ell$ are generated identically in $\mathsf{Hybrid}_1$ and $\mathsf{Hybrid}_2$. We prove that $\mathsf{Hybrid}_1 \approx_{\mathsf{poly}(n \cdot 2^y)} \mathsf{Hybrid}_2$ by $\mathsf{poly}(n \cdot 2^y)$ non-malleability of the underlying commitment scheme $\mathsf{Com}$.

To this end, suppose there exists a $\mathsf{poly}(n \cdot 2^y)$-time distinguisher that distinguishes $\mathsf{Hybrid}_1$ and $\mathsf{Hybrid}_2$ with advantage $1/\mathsf{poly}(n \cdot 2^y)$ (for infinitely many $n \in \mathbb{N}$). We will use this distinguisher to contradict $kt/2$-to-$ky$ same-tag auxiliary-input non-malleability w.r.t. replacement of $\mathsf{Com}$ against $\mathsf{poly}(n \cdot 2^y)$-size adversaries, according to Definition 3, as follows.

We define auxiliary-input functions $\{\mathsf{au}_{\lambda,j}\}_{\lambda \in [t/2], j \in [k]}$, an adversary $\mathcal{A}'$, and messages and tags corresponding to the underlying commitment scheme $\mathsf{Com}$. These are defined identically to the ones defined in the description of $\mathcal{V}_{\beta,\mathsf{real}}$ and $\mathcal{V}_{\beta,\mathsf{ideal}}$. We recall the definitions below.

1. We define $\{\mathsf{au}_{\lambda,j}\}_{\lambda \in [t/2], j \in [k]}$ as follows:
   (a) For each $j' \in [k]$, define an auxiliary input function $\mathsf{au}_{j'}$ that on input
   $$\left(\{C'_{\lambda,j}, s'_\lambda\}_{\lambda \in [t/2], j \in [k]}, \{M'_{\lambda,j}\}_{\lambda \in [t/2], j \in [k] \setminus \{j'\}}, \{r'_{\lambda,j}\}_{\lambda \in [t/2], j \in [k] \setminus \{j'\}}\right),$$
   sets
   $$X = \{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda \in [t/2], j \in [k]} \text{ and } W = \left([k] \setminus \{j'\}, \{M_{\lambda,j}, r_{\lambda,j}\}_{\lambda \in [t/2], j \in [k] \setminus \{j'\}}\right).$$
   If $R_L(X, W) = 1$, then it outputs a NIWI for the statement $X \in L$[20], else it outputs $\perp$.
   (b) For all $\lambda \in [t/2]$ and $j \in [k]$, set $\mathsf{au}_{\lambda,j} = \mathsf{au}_j$[21].

[20] Refer to Figure 2 for a description of the language $L$.
[21] Note that $\mathsf{au}_{\lambda,j}$ takes as input additional messages and randomness which he ignores.

2. We define adversary $\mathcal{A}'$ that has $\beta, m_1, \ldots m_\ell, \mathsf{tag}_1, \ldots \mathsf{tag}_\ell$ hardwired, and on input

$$\left(\{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}'\right),$$

does the following:

   (a) Sample $r_1, \ldots r_\ell \xleftarrow{\$} \{0,1\}^*$.
   (b) For all $i \in [\ell] \setminus \{\beta\}$, generate $c_i$ using randomness $r_i$, according to the distribution of $c_{\beta-1,i}$ defined above.
   (c) Set $c_\beta = \left(\mathsf{tag}_\beta, \{(C'_{\lambda,j}, s'_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}'\right)$.
   (d) Compute $\mathsf{a}_\beta = \mathsf{aux}_\beta(c_1, \ldots c_\ell, (0^p)_{\times(\beta-1)}, m_{\beta+1}, \ldots m_\ell, r_1, \ldots r_{\beta-1}, r_{\beta+1}, \ldots r_\ell)$.
   (e) Execute $\mathcal{A}(c_1, \ldots, c_\ell, \mathsf{a}_\beta)$ to obtain $(\widetilde{c}_1, \ldots \widetilde{c}_y, z)$.
   (f) Set $Z = (z, c_1, \ldots, c_\beta, c_{\beta+1}, \ldots, c_\ell, \widetilde{c}_1, \ldots, \widetilde{c}_y)$.
   (g) For each $i \in [y]$, parse $\widetilde{c}_i = (\widetilde{\mathsf{tag}}, \{(\widetilde{C}^i_{\lambda,j}, \widetilde{s}_\lambda)\}_{\lambda\in[t/2],j\in[k]}, \Pi_i)$.
   (h) Output $\left(\{(\widetilde{C}^i_{\widetilde{\lambda}_\beta,j}, \widetilde{s}_{\widetilde{\lambda}_\beta})\}_{i\in[y],j\in[k]}, Z\right)$.

3. For all $\lambda \in [t/2]$ and $j \in [k]$, set $m_{\lambda,j} = m_\beta$.

4. For all $\lambda \in [t/2]$ and $j \in [k]$, set $s_{\lambda,j} = s'_\lambda$, where $\{s'_\lambda\}_{\lambda\in[t/2]}$ are the input tags.

Note that $\{m_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{s_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{\mathsf{au}_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}$, as defined above, satisfy Equation (1) (Definition 3), corresponding to the underlying commitment Com. Therefore, for

$$\{m_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{s_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \{\mathsf{au}_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \mathcal{A}'$$

there exist distributions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$, which we denote by $v_{\mathsf{Real}}$ and $v_{\mathsf{Ideal}}$, such that:

$$(\tau_0, v_{\mathsf{Real}}(\tau_0)) \approx_{\mathsf{poly}(n\cdot 2^y)} (\tau_{kt/2}, v_{\mathsf{Ideal}}(\tau_{kt/2})) \tag{4}$$

where $\tau_0 = \left(\{C^0_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}^0, \mathcal{A}'(\{C^0_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}^0)\right)$ is such that for every $\lambda \in [t/2], j \in [k]$,

- $r_{\lambda,j} \xleftarrow{\$} \{0,1\}^*$,
- $C^0_{\lambda,j} = \mathsf{Com}_{\mathsf{tag}_{\lambda,j}}(m_\beta, r_{\lambda,j})$, and
- $\mathsf{au}^0 = \mathsf{au}_{kt/2}\left(\{C^0_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, (m_\beta)_{\times(kt/2-1)}, \{r_{\lambda,j}\}_{(\lambda,j)\in[t/2]\times[k]\setminus\{(t/2,k)\}}\right)$.

Similarly, $\tau_{kt/2} = \left(\{C^{kt/2}_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}^{kt/2}, \mathcal{A}'(\{C^{kt/2}_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, \mathsf{au}^{kt/2})\right)$ is such that for every $\lambda \in [t/2], j \in [k]$,

- $r_{\lambda,j} \xleftarrow{\$} \{0,1\}^*$,
- $C^{kt/2}_{\lambda,j} = \mathsf{Com}_{\mathsf{tag}_{\lambda,j}}(0^p, r_{\lambda,j})$, and
- $\mathsf{au}^{kt/2} = \mathsf{au}_{t/2,k}\left(\{C^0_{\lambda,j}\}_{\lambda\in[t/2],j\in[k]}, (0)_{\times(kt/2-1)}, \{r_{\lambda,j}\}_{(\lambda,j)\in[t/2]\times[k]\setminus\{(t/2,k)\}}\right)$.

Note that $\mathsf{Hybrid}_1$ outputs

$$(c_{\beta-1,1},\ldots,c_{\beta-1,\ell},\mathsf{a}_\beta,\widetilde{c}_1,\ldots,\widetilde{c}_y,z,v_{\mathsf{Real}}(\tau_0))$$

which is efficiently computable from

$$(\tau_0,v_{\mathsf{Real}}(\tau_0))\,.$$

Similarly, $\mathsf{Hybrid}_2$ outputs

$$\left(c_{\beta,1},\ldots,c_{\beta,\ell},\mathsf{a}_\beta,\widetilde{c}_1,\ldots,\widetilde{c}_y,z,v_{\mathsf{Ideal}}(\tau_{tk/2})\right)$$

which is efficiently computable from

$$\left(\tau_{kt/2},v_{\mathsf{Ideal}}(\tau_{kt/2})\right).$$

Therefore, if there exists a $\mathsf{poly}(n\cdot 2^y)$-time distinguisher $\mathcal{D}$ such that for infinitely many $n\in\mathbb{N}$

$$\left|\Pr[\mathcal{D}(\mathsf{Hybrid}_1)=1]-\Pr[\mathcal{D}(\mathsf{Hybrid}_2)=1]\right|\geq\frac{1}{\mathsf{poly}(n\cdot 2^y)},$$

then there exists a $\mathsf{poly}(n\cdot 2^y)$-time distinguisher $\mathcal{D}'$ such that for infinitely many $n\in\mathbb{N}$

$$\left|\Pr[\mathcal{D}'\left(\tau_0,v_{\mathsf{Real}}(\tau_0)\right)=1]-Pr[\mathcal{D}'\left(\tau_{t/2,k},v_{\mathsf{Ideal}}(\tau_{t/2,k})\right)=1]\right|\geq\frac{1}{\mathsf{poly}(n\cdot 2^y)}$$

contradicing Equation (4), as desired.

These two hybrids prove that

$$\left(\tau_{\beta-1},\mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\right)\approx_{\mathsf{poly}(n\cdot 2^y)}\left(\tau_\beta,\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\right),$$

completing the proof of the lemma. □

It is tempting to try to prove that for every $\beta\in[\ell-1]$,

$$\left(\tau,\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)\right)\approx\left(\tau,\mathcal{V}_{\beta+1,\mathsf{real}}(\tau)\right),\tag{5}$$

and then use Lemma 1, together with a standard hybrid argument, to argue that

$$\left(\tau_0,\mathcal{V}_{1,\mathsf{real}}(\tau_0)\right)\approx\left(\tau_\ell,\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\ell)\right),$$

and thus define $\mathcal{V}_{\mathsf{Real}}$ according to $\left(\tau_0,\mathcal{V}_{1,\mathsf{real}}(\tau_0)\right)$, while converting each $(\widetilde{M}_i,\psi_i)$ to $\widetilde{M}_i$; and similarly, define $\mathcal{V}_{\mathsf{Ideal}}$ according to $\left(\tau_\ell,\mathcal{V}_{\ell,\mathsf{ideal}}(\tau_\ell)\right)$, while converting each $(\widetilde{M}_i,\psi_i)$ to $\widetilde{M}_i$.

Unfortunately, Equation (5) is not necessarily true. Equation (5) is true if we assume the adversary always generates valid commitments. However, for a general adversary, it may be the case that $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)$ outputs $\perp$, whereas $\mathcal{V}_{\beta+1,\mathsf{real}}(\tau)$ does not. The reason is two-fold: First, $\mathcal{V}_{\beta+1,\mathsf{real}}$ extracts the commitments corresponding to $\widetilde{s}_{\widetilde{\lambda}_{\beta+1}}$ whereas $\mathcal{V}_{\beta,\mathsf{ideal}}$ extracts the commitments corresponding to $\widetilde{s}_{\widetilde{\lambda}_\beta}$. Second, $\mathcal{V}_{\beta+1,\mathsf{real}}$ is "more forgiving" than $\mathcal{V}_{\beta,\mathsf{ideal}}$.

Jumping ahead, to make the distributions $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)$ and $\mathcal{V}_{\beta+1,\mathsf{real}}(\tau)$ indistinguishable, we need to sometimes convert the output of $\mathcal{V}_{\beta+1,\mathsf{real}}(\tau)$ to $\perp$. We do this by using the leakage lemma due to Gentry and Wichs [GW11], as follows.

In the next part of the proof, we fix any $\beta \in [\ell - 1]$ and consider the distributions $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)$ and $\mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta)$.

In what follows, we consider an arbitrary transcript $\tau$, and for any $\beta \in [\ell - 1]$ and any $i \in [y]$, we denote the output of $\mathcal{V}_{\beta,\mathsf{ideal}}(\tau)$ by $(\chi_1, \ldots \chi_y)$, and denote by $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau)$ the value $\chi_i$. Similarly, we denote the output of $\mathcal{V}_{\beta+1,\mathsf{real}}(\tau)$ by $(\chi_1, \ldots \chi_y)$, and denote by $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau)$ the value $\chi_i$. Note that the output $\chi_i$ of $\mathcal{V}^i_{\beta,\mathsf{ideal}}$ only depends on values $\{\widetilde{M}_{\widetilde{\lambda}_\beta,j}\}_{j\in[k]}$ corresponding to the $i^{th}$ right commitments with (small) tag $\widetilde{s}_{\widetilde{\lambda}_\beta} \notin \{s_{1,\beta}, \ldots s_{\ell,\beta}\}$, whereas the output $\chi_i$ of $\mathcal{V}^i_{\beta+1,\mathsf{real}}$ only depends on the values $\{\widetilde{M}_{\widetilde{\lambda}_{\beta+1},j}\}_{j\in[k]}$ corresponding to the $i^{th}$ commitments with (small) tag $\widetilde{s}_{\widetilde{\lambda}_{\beta+1}} \notin \{s_{1,\beta+1}, \ldots s_{\ell,\beta+1}\}$.

Note that since $\mathsf{REJECT}$ is efficiently computable, if $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) = \mathsf{REJECT}$ then $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = \mathsf{REJECT}$. Moreover, if $\Pi_i$ is an accepting proof, then by the soundness of the NIWI proof system,[22] $\{\widetilde{M}_{\widetilde{\lambda}_\beta,j}\}_{j\in[k]}$ and $\{\widetilde{M}_{\widetilde{\lambda}_{\beta+1},j}\}_{j\in[k]}$ in the $i^{th}$ commitment share at least $(k-1)$ elements. Therefore, by the soundness of the NIWI, the following holds for all $\tau$, where $\tau = (c_1, \ldots c_\ell, \widetilde{c}_1, \ldots \widetilde{c}_y, z)$ denotes any transcript of an execution.

1. $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) = (\widetilde{M}, \psi)$ for $\psi \in \left[\left(\frac{3k}{4} + 1 - \beta\right), k\right] \implies$
   $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = (\widetilde{M}, \psi')$ where $\psi' \in \{\psi - 1, \psi, \psi + 1\}$ and $\psi' \leq k$.
2. $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) = \perp \implies \mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) \in \{\perp\} \cup \{(\widetilde{M}, \psi')\}_{\widetilde{M}\in\{0,1\}^{p(n)}}$ for $\psi' \in \left\{\left(\frac{3k}{4} - \beta\right), \left(\frac{3k}{4} - \beta + 1\right)\right\}$.

Next we prove that if $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) \neq \perp$, then one can efficiently compute $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau)$ from $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau)$ given only 2 additional bits of (inefficient) leakage. To this end, we define an (inefficient) leakage function $\pi^i_\beta(\cdot)$ with range $\{0, -1, 1, *\}$, and an efficient function $f^i$ such that for every transcript $\tau$,

$$\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = f^i(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau), \pi^i_\beta(\tau)) \tag{6}$$

whenever $\pi^i_\beta(\tau) \neq *$.

Intuitively, the leakage value 0 indicates that $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau)$ is identical to $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau)$. The leakage values $\{-1, 1\}$ indicate that $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau)$ contains some message and value $\psi$, and $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau)$ contains the same message and $\psi \pm 1$. The leakage value $*$ indicates failure. We formally define $\pi^i_\beta$ and $f^i$ in Figure 3.

Note that the leakage $\pi_\beta$ consists of $2y$ bits. Recall that by Lemma 1, the distributions $\left(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\right)$ and $\left(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\right)$ are $\mathsf{poly}(n \cdot 2^y)$-indistinguishable. Therefore, we can rely on the Gentry-Wichs leakage lemma [GW11] (stated below, and adapted to our regime) to argue that there exists an augmentation function $\widehat{\pi}_{\beta-1}$ such that

$$\left(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1}), \pi_{\beta-1}(\tau_{\beta-1})\right) \approx \left(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta), \widehat{\pi}_{\beta-1}(\tau_\beta)\right).$$

**Lemma 2.** *[GW11, JP14, CLP15] Let $X$ and $Y$ be any two distributions that cannot be distinguished with advantage more than $\epsilon$ by machines of size $T$. Then, for any leakage function $\pi$ that outputs $\gamma$ bits, there exists a function $\widehat{\pi}$ such that*

$$\left(x, \pi(x)\right) \text{ and } \left(y, \widehat{\pi}(y)\right) \text{ for } x \leftarrow X \text{ and } y \leftarrow Y$$

[22] For simplicity, we rely on deterministically verifiable NIWIs. Known NIWIs [BOV07, GOS12] satisfy this condition.

1. $\Pi_i$ rejects $\iff \mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta) = \mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau_\beta) = \mathsf{REJECT}$.
2. If $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) = (\widetilde{M}, \psi)$ and $\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = (\widetilde{M}, \psi')$ then
   - Set $\pi^i_\beta(\tau) = \psi' - \psi$[a].
   - Define $f^i((\widetilde{M}, \psi), \Pi) = (\widetilde{M}, \psi + \Pi)$ if $\Pi \in \{-1, 0, 1\}$ and $f^i((\widetilde{M}, \psi), *) = \perp$.[b]
3. If $\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau) = \perp$ then set
   - Set $\pi^i_\beta(\tau) = 0 \iff \mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = \perp$
   - Set $\pi^i_\beta(\tau) = * \iff \mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau) = (M, \frac{3k}{4} - \beta + b)$ for $b \in \{0, 1\}$.
   - Define $f^i(\perp, \cdot) = \perp$.

**Defining $\pi_\beta$.** Define $\pi_\beta = (\pi^1_\beta, \pi^2_\beta, \ldots, \pi^y_\beta)$.
**Defining $f$.** Define $f\Big((\chi_1, \ldots \chi_y), \pi_\beta(\tau)\Big) = (\chi'_1, \ldots, \chi'_y)$, where $\chi'_i = f^i(\chi_i, \pi^i_\beta(\tau))$.

[a] Note that $\psi' = (\psi \pm 1)$.
[b] We note that in this case, $\Pi \neq *$, but we define $f$ on the entire domain for completeness.

Figure 3: The definition of $\pi_\beta$ and $f$.

*cannot be distinguished with advantage more than $2\epsilon$, by machines of size $\left(\frac{\epsilon^4 T}{2^\gamma \cdot \log T}\right)^{\frac{1}{3}}$.*[23]

*Furthermore, if $X \approx_{\mathsf{poly}(T)} Y$ and $H_\infty(X), H_\infty(Y) \geq \omega(\log(T) + \log^2(n))$, then in time $2^{O(\gamma)} \cdot \big(n \cdot T\big)^{\log n}$ one can compute $\widehat{\pi}$ for which*

$$\Big(x, \pi(x)\Big) \approx_{\mathsf{poly}(T/2^\gamma)} \Big(y, \widehat{\pi}(y)\Big).$$

We next describe how we use Lemma 1 and Lemma 2 to complete the proof of Theorem 2. Recall that in order to show that the scheme in Figure 2 satisfies Definition 3, we need to define $\mathcal{V}_{\mathsf{real}}$ and $\mathcal{V}_{\mathsf{ideal}}$ and prove that $\Big(\tau_0, \mathcal{V}_{\mathsf{real}}(\tau_0)\Big) \approx \Big(\tau_\ell, \mathcal{V}_{\mathsf{Ideal}}(\tau_\ell)\Big)$.

**First attempt at defining $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$.**

For simplicity, we assume that $\pi^i_\beta(\tau_\beta) \neq *$ for every $i \in [y]$ and every $\beta \in [1, \ell]$.

Fix any $\beta \in [\ell]$. By Lemma 1,

$$\Big(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\Big) \approx_{\mathsf{poly}(n \cdot 2^y)} \Big(\tau_{\beta-1}, \mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1})\Big). \tag{7}$$

By Equation (6), with our simplifying assumption,

$$\mathcal{V}_{\beta,\mathsf{real}}(\tau_{\beta-1}) = f(\mathcal{V}_{\beta-1,\mathsf{ideal}}(\tau_{\beta-1}), \pi_{\beta-1}(\tau_{\beta-1})). \tag{8}$$

[23] Note that this statement is not asymptotic. In the next sentence we state an asymptotic version that suffices for our applications.

Combining Equation (7) and Equation (8),

$$\Big(\tau_\beta, \mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_{\beta-1}, f\big(\mathcal{V}_{\beta-1,\mathsf{ideal}}(\tau_{\beta-1}), \pi_{\beta-1}(\tau_{\beta-1})\big)\Big). \tag{9}$$

Setting $\beta = \ell$ in Equation (9),

$$\Big(\tau_\ell, \mathcal{V}_{\ell,\mathsf{ideal}}(\tau_\ell)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_{\ell-1}, f\big(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \pi_{\ell-1}(\tau_{\ell-1})\big)\Big). \tag{10}$$

**We will denote the left hand side of Equation (10) by $J_\ell(\tau_\ell)$, and the right hand side by $J_{\ell-1}(\tau_{\ell-1})$.** Thus,

$$J_\ell(\tau_\ell) \approx_{\mathsf{poly}(n\cdot 2^y)} J_{\ell-1}(\tau_{\ell-1}).$$

Next, we will derive a sequence $J_{\ell-2}(\tau_{\ell-2}), J_{\ell-3}(\tau_{\ell-3}), \ldots, J_1(\tau_1), J_0(\tau_0)$, and prove that for every $\alpha \in [\ell-1, \ldots, 0]$,

$$J_{\alpha+1}(\tau_{\alpha+1}) \approx J_\alpha(\tau_\alpha).$$

To this end, setting $\beta = \ell - 1$ in Equation (9),

$$\Big(\tau_{\ell-1}, \mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1})\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_{\ell-2}, f\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\big)\Big). \tag{11}$$

Since the output of $\pi_{\ell-1}$ consists of $2y$ bits, set $\widehat{\pi}_{\ell-1}$ according to the leakage lemma (Lemma 2) for Equation (11) so that:

$$\Big(\tau_{\ell-1}, \mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \pi_{\ell-1}(\tau_{\ell-1})\Big) \approx \Big(\tau_{\ell-2}, f\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\big), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\Big). \tag{12}$$

**Remark 5.** *We note that according to Lemma 2, the leakage $\widehat{\pi}_{\ell-1}$ is a function of $(\tau_{\ell-2}, \mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}))$ and not only of $\tau_{\ell-2}$. However, to avoid cluttering of notation, we denote $\widehat{\pi}_{\ell-1}(\tau_{\ell-2}, \mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}))$ by $\widehat{\pi}_{\ell-1}(\tau_{\ell-2})$. We use similar notation throughout the proof.*

Because $f$ is an efficient function, we can apply it to Equation (12) so that:

$$\Big(\tau_{\ell-1}, f\big(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \pi_{\ell-1}(\tau_{\ell-1})\big)\Big) \approx \Big(\tau_{\ell-2}, f\big(f\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\big), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\big)\Big). \tag{13}$$

Define $\eta_{\ell-2}(\cdot)$ and $h(\cdot)$ such that for all $\tau$ and all $i \in [y]$[24],

$$\text{If } \pi^i_{\ell-2}(\tau) = * \text{ or } \widehat{\pi}^i_{\ell-1}(\tau) = *, \text{ set } \eta^i_{\ell-2}(\tau) = *.$$

$$\text{Else, set } \eta^i_{\ell-2}(\tau) = \pi^i_{\ell-2}(\tau) + \widehat{\pi}^i_{\ell-1}(\tau).$$

$$h^i((\widetilde{M}, \psi), \eta) = (\widetilde{M}, \psi + \eta) \text{ if } \eta \neq *, \text{ and } h^i(\perp, \cdot) = h^i(\cdot, *) = \perp.$$

Note that

$$f\big(f\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\big), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\big) = h\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\big)$$

Substituting into Equation (13), we have:

$$\Big(\tau_{\ell-1}, f\big(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \pi_{\ell-1}(\tau_{\ell-1})\big)\Big) \approx \Big(\tau_{\ell-2}, h\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\big)\Big). \tag{14}$$

**We denote the right hand side of Equation (14) by $J_{\ell-2}(\tau_{\ell-2})$.**

[24] We note that $h$ is identical to $f$, except that it operates over a larger leakage domain.

Note that the left hand side of the Equation (14) is $J_{\ell-1}(\tau_{\ell-1})$, and thus

$$J_{\ell-1}(\tau_{\ell-1}) \approx J_{\ell-2}(\tau_{\ell-2}).$$

Next, setting $\beta = (\ell - 2)$ in Equation (9) we have:

$$\Big(\tau_{\ell-2}, \mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2})\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_{\ell-3}, f\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\big)\Big). \tag{15}$$

Since the output of $\eta_{\ell-2}$ consists of $O(y)$ bits, set $\widehat{\eta}_{\ell-2}$ according to the leakage lemma (Lemma 2) for Equation (15) so that:

$$\Big(\tau_{\ell-2}, \mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\Big) \approx \Big(\tau_{\ell-3}, f\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\big), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\Big). \tag{16}$$

Because $h$ is an efficient function, applying it to both sides of the equation above:

$$\Big(\tau_{\ell-2}, h(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2}))\Big) \approx \Big(\tau_{\ell-3}, h\big(f\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\big), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\big)\Big). \tag{17}$$

Define $\eta_{\ell-3}(\cdot)$ such that for all $\tau$ and all $i \in [y]$,

$$\text{If } \pi^i_{\ell-3}(\tau) = * \text{ or } \widehat{\eta}^i_{\ell-2}(\tau) = *, \text{ set } \eta^i_{\ell-3}(\tau) = *,$$

$$\text{Else set } \eta^i_{\ell-3}(\tau) = \pi^i_{\ell-3}(\tau) + \widehat{\eta}^i_{\ell-2}(\tau).$$

$$\text{Note that } h^i((\widetilde{M}, \psi), \eta) = (\widetilde{M}, \psi + \eta) \text{ if } \eta \neq *, \text{ and } h^i(\perp, \cdot) = h^i(\cdot, *) = \perp.$$

Therefore,

$$h\big(f\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\big), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\big) = h\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \eta_{\ell-3}(\tau_{\ell-3})\big).$$

Substituting into Equation (17), we have:

$$\Big(\tau_{\ell-2}, h\big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\big)\Big) \approx \Big(\tau_{\ell-3}, h\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \eta_{\ell-3}(\tau_{\ell-3})\big)\Big) \tag{18}$$

**We denote the right hand side of Equation (18) by $J_{\ell-3}(\tau_{\ell-3})$.**

Note that the left hand side of the Equation (18) is $J_{\ell-2}(\tau_{\ell-2})$, and thus

$$J_{\ell-2}(\tau_{\ell-2}) \approx J_{\ell-3}(\tau_{\ell-3}).$$

Similarly, for all $\alpha \in [1, \ell - 4]$, we define $\eta_\alpha(\cdot)$ that outputs $O(y \cdot \log \ell)$ bits, and define

$$J_\alpha(\tau_\alpha) \triangleq h\big(\mathcal{V}_{\alpha,\mathsf{ideal}}(\tau_\alpha), \eta_\alpha(\tau_\alpha)\big).$$

The same argument as above implies that for every $\alpha \in [\ell - 1]$,

$$(\tau_{\alpha+1}, J_{\alpha+1}(\tau_{\alpha+1})) \approx (\tau_\alpha, J_\alpha(\tau_\alpha)).$$

This follows by setting $\beta = (\alpha + 1)$ in Equation (9), and then applying the sequence of Equations (16, 17, 18) with $(\alpha + 1)$ instead of $(\ell - 2)$.

Therefore, we conclude that

$$(\tau_\ell, J_\ell(\tau_\ell)) \approx (\tau_1, J_1(\tau_1)). \tag{19}$$

Recall that we need to prove that

$$(\tau_\ell, J_\ell(\tau_\ell)) \approx (\tau_0, J_0(\tau_0))\,,$$

for some $J_0$, which we define next. To this end, by Lemma 1 (for $\beta = 1$):

$$\Big(\tau_1, \mathcal{V}_{1,\mathsf{ideal}}(\tau_1)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_0, \mathcal{V}_{1,\mathsf{real}}(\tau_0)\Big). \tag{20}$$

Set $\widehat{\eta}_1$ according to the leakage lemma (Lemma 2) for Equation (20),

$$\Big(\tau_1, \mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)\Big) \approx \Big(\tau_0, \mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)$$

Because $h$ is an efficient function,

$$\Big(\tau_1, h\big(\mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)\big)\Big) \approx \Big(\tau_0, h\big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\big)\Big). \tag{21}$$

Thus,

$$\Big(\tau_1, J_1(\tau_1)\Big) \approx \Big(\tau_0, h\big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\big)\Big) \triangleq \Big(\tau_0, J_0(\tau_0)\Big), \tag{22}$$

which together with Equation (19), implies that

$$\Big(\tau_\ell, J_\ell(\tau_\ell)\Big) \approx \Big(\tau_0, J_0(\tau_0)\Big), \tag{23}$$

as desired.

Thus, under the assumption that $(\pi^i_\beta \neq *)$ for all $i \in [y]$ and all $\beta \in [1, \ell-1]$, we can define $F$ as a function that on input a tuple $(\chi_1, \ldots, \chi_y)$ outputs $(\widetilde{m}_1, \ldots, \widetilde{m}_y)$ such that for all $i \in [y]$, if $\chi_i = (\widetilde{M}, \psi)$ for some $\widetilde{M} \in \{0,1\}^p$ and some $\psi \geq 0$, then $\widetilde{m}_i = \widetilde{M}$, else $\widetilde{m}_i = \perp$. We can then define,

$$\mathcal{V}_{\mathsf{Real}}(\tau_0) = F(J_0(\tau_0))$$

and

$$\mathcal{V}_{\mathsf{Ideal}}(\tau_\ell) = F(J_\ell(\tau_\ell))$$

and by Equation (23) conclude that

$$\Big(\tau_0, \mathcal{V}_{\mathsf{Real}}(\tau_0)\Big) \approx \Big(\tau_\ell, \mathcal{V}_{\mathsf{Ideal}}(\tau_\ell)\Big),$$

as desired.

However, the assumption that $\pi^i_\beta \neq *$ for all $i \in [y]$ and all $\beta \in [1, \ell-1]$, is not necessarily true. In what follows, we remove this assumption. To that end, we need to define the distributions $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ differently, to ensure indistinguishability even when for some $\beta \in [1, \ell-1]$ and some $i \in [y]$, $\pi^i_\beta = *$.

**Defining $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ in the general case.**
Note that if $\pi^i_\beta(\tau_\beta) \neq *$ for all $i \in [y]$, then Equation (8) holds. However, if $\pi^i_\beta(\tau_\beta) = *$ for some $i \in [y]$, then Equation (8) does not hold. In this case,

$$\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau_\beta) = (\widetilde{M}, \frac{3k}{4} - \beta + b) \text{ for some } \widetilde{M} \text{ and some } b \in \{0,1\}, \text{ whereas}$$

$$f^i(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \pi^i_\beta(\tau_\beta)) = \perp.$$

We next define an efficient function $g$ and inefficient leakage functions $\phi_\beta$ for every $\beta \in [1, \ell-1]$, such that $g$ applied to $\mathcal{V}_{\beta+1}$ sometimes changes a value $(\widetilde{M}, \frac{3k}{4} - \beta + b)$ to $\perp$, ensuring that

$$g(\mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta), \phi_\beta(\tau_\beta)) = f(\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta), \pi_\beta(\tau_\beta)). \tag{24}$$

To this end, we define the leakage function $\phi_\beta = (\phi_\beta^1, \ldots \phi_\beta^y)$ such that for every $i \in [y]$ and every transcript $\tau$,

- $(\phi_\beta^i(\tau) = *) \iff (\pi_\beta^i(\tau) = *)$.
- $\phi_\beta^i(\tau) = 0$ otherwise.

Define the function $g$ that takes input $x$ and $\Phi \in \{0, *\}$ such that for all $x$,

- $g(x, 0) = x$,
- $g(x, *) = \perp$.

For any $\mathcal{X} = (\chi_1, \ldots, \chi_y)$ and any leakage value $\Phi \in \{0,*\}^y$, define $\chi_i' \triangleq g(\chi_i, \Phi_i)$ and set $g(\mathcal{X}, \Phi) = (\chi_1' \ldots, \chi_y')$ [25]. Note that for every $\beta \in [1, \ell-1]$, the functions $g$ and $\phi_\beta$ defined above, satisfy Equation (24), as desired.
Recall that by Lemma 1, for every $\beta \in [0, \ell-1]$,

$$\Big(\tau_{\beta+1}, \mathcal{V}_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}),\Big) \approx_{\mathsf{poly}(n \cdot 2^y)} \Big(\tau_\beta, \mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta)\Big).$$

We set $\widehat{\phi}_\beta$ according to the leakage lemma (Lemma 2)[26], so that

$$\Big(\tau_{\beta+1}, \mathcal{V}_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \widehat{\phi}_\beta(\tau_{\beta+1})\Big) \approx_{\mathsf{poly}(n \cdot 2^y)} \Big(\tau_\beta, \mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta), \phi_\beta(\tau_\beta)\Big), \tag{25}$$

and rely on the fact that $g$ is efficiently computable, to conclude that for all $\beta \in [1, \ell-1]$:

$$\begin{aligned}
&\Big(\tau_{\beta+1}, g(\mathcal{V}_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \widehat{\phi}_\beta(\tau_{\beta+1}))\Big) \approx_{\mathsf{poly}(n \cdot 2^y)} \\
&\Big(\tau_\beta, g(\mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta), \phi_\beta(\tau_\beta))\Big) = \\
&\Big(\tau_\beta, f(\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta), \pi_\beta(\tau_\beta))\Big).
\end{aligned} \tag{26}$$

Setting $\beta = \ell - 1$ in Equation (26), we have:

$$\Big(\tau_\ell, g(\mathcal{V}_{\ell,\mathsf{ideal}}(\tau_\ell), \widehat{\phi}_{\ell-1}(\tau_\ell))\Big) \approx_{\mathsf{poly}(n \cdot 2^y)} \Big(\tau_{\ell-1}, f\big(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \pi_{\ell-1}(\tau_{\ell-1})\big)\Big). \tag{27}$$

Setting $\beta = (\ell - 2)$ in Equation (26),

$$\left(\tau_{\ell-1}, g\Big(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \widehat{\phi}_{\ell-2}(\tau_{\ell-1})\Big)\right) \approx_{\mathsf{poly}(n \cdot 2^y)} \left(\tau_{\ell-2}, f\Big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\Big)\right) \tag{28}$$

[25] Here, we overload notation and allow $g$ to take as input an individual pair $\chi$ or a tuple of pairs $(\chi_1, \ldots \chi_y)$.
[26] Note that when applying Lemma 2, we have a $\mathsf{poly}(n \cdot 2^y)$ loss in security. Therefore, this usage cannot be made repeatedly, more than a constant number of times. This is the first application, and we will use this lemma three times.

Since $\pi_{\ell-1}$ outputs $2y$ bits, we will set $\widehat{\pi}_{\ell-1}$ according to the leakage lemma (Lemma 2)[27] for Equation (28) such that

$$\left(\tau_{\ell-1}, g\left(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \widehat{\phi}_{\ell-2}(\tau_{\ell-1})\right), \pi_{\ell-1}(\tau_{\ell-1})\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_{\ell-2}, f\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\right), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\right)$$

Because the function $f$ is efficient, we conclude that

$$\left(\tau_{\ell-1}, f\left(g\left(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \widehat{\phi}_{\ell-2}(\tau_{\ell-1})\right), \pi_{\ell-1}(\tau_{\ell-1})\right)\right) \approx_{\mathsf{poly}(n\cdot 2^y)}$$
$$\left(\tau_{\ell-2}, f\left(f\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\right), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\right)\right)$$

We define $\eta_{\ell-2}$ exactly as before, such that for all $\tau$ and all $i \in [y]$,

$$\eta^i_{\ell-2}(\tau) = * \iff \pi^i_{\ell-2}(\tau) = * \text{ or } \widehat{\pi}^i_{\ell-1}(\tau) = *$$

$$\text{Else, } \eta^i_{\ell-2}(\tau) = \pi^i_{\ell-2}(\tau) + \widehat{\pi}^i_{\ell-1}(\tau).$$

$$\text{Recall that } h^i((\widetilde{M}, \psi), \eta) = (\widetilde{M}, \psi + \eta) \text{ if } \eta \neq *, \text{ and } h^i(\perp, \cdot) = h^i(\cdot, *) = \perp.$$

By definition,

$$f\left(f\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \pi_{\ell-2}(\tau_{\ell-2})\right), \widehat{\pi}_{\ell-1}(\tau_{\ell-2})\right) = h\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\right).$$

Thus,

$$\left(\tau_{\ell-1}, f\left(g\left(\mathcal{V}_{\ell-1,\mathsf{ideal}}(\tau_{\ell-1}), \widehat{\phi}_{\ell-2}(\tau_{\ell-1})\right), \pi_{\ell-1}(\tau_{\ell-1})\right)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_{\ell-2}, h\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \eta_{\ell-2}(\tau_{\ell-2})\right)\right) \tag{29}$$

Similarly, setting $\beta = (\ell - 3)$ in Equation (26),

$$\left(\tau_{\ell-2}, g\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \widehat{\phi}_{\ell-3}(\tau_{\ell-2})\right)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_{\ell-3}, f\left(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\right)\right) \tag{30}$$

Since $\eta_{\ell-2}$ outputs $O(y)$ bits, we will set $\widehat{\eta}_{\ell-2}$ according to the leakage lemma (Lemma 2)[28] for Equation (30) such that

$$\left(\tau_{\ell-2}, g\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \widehat{\phi}_{\ell-3}(\tau_{\ell-2})\right), \eta_{\ell-2}(\tau_{\ell-2})\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_{\ell-3}, f\left(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\right), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\right) \tag{31}$$

Because the function $h$ is efficient, we conclude that

$$\left(\tau_{\ell-2}, h\left(g\left(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \widehat{\phi}_{\ell-3}(\tau_{\ell-2})\right), \eta_{\ell-2}(\tau_{\ell-2})\right)\right) \approx_{\mathsf{poly}(n\cdot 2^y)}$$
$$\left(\tau_{\ell-3}, h\left(f\left(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\right), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\right)\right) \tag{32}$$

[27] This is the second sequential application of the leakage lemma.
[28] This is the second sequential application of the leakage lemma.

We define $\eta_{\ell-3}$ exactly as before such that for all $\tau$ and all $i \in [y]$,

$$\eta_{\ell-3} = * \iff \pi^i_{\ell-3} = * \text{ or } \widehat{\eta}^i_{\ell-2}(\tau) = *, \text{ and}$$

$$\eta^i_{\ell-3}(\tau) = \pi^i_{\ell-3}(\tau) + \widehat{\eta}^i_{\ell-2}(\tau).$$

Recall that $h^i((\widetilde{M}, \psi), \eta) = (\widetilde{M}, \psi + \eta)$ if $\eta \neq *$, and $h^i(\bot, \cdot) = h^i(\cdot, *) = \bot$.

By definition,

$$\Big(\tau_{\ell-3}, h\big(f\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \pi_{\ell-3}(\tau_{\ell-3})\big), \widehat{\eta}_{\ell-2}(\tau_{\ell-3})\big)\Big) = \Big(\tau_{\ell-3}, h\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \eta_{\ell-3}(\tau_{\ell-3})\big)\Big) \quad (33)$$

Therefore,

$$\left(\tau_{\ell-2}, h\Big(g\Big(\mathcal{V}_{\ell-2,\mathsf{ideal}}(\tau_{\ell-2}), \widehat{\phi}_{\ell-3}(\tau_{\ell-2})\Big), \eta_{\ell-2}(\tau_{\ell-2})\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_{\ell-3}, h\big(\mathcal{V}_{\ell-3,\mathsf{ideal}}(\tau_{\ell-3}), \eta_{\ell-3}(\tau_{\ell-3})\big)\Big) \quad (34)$$

Similarly, for all $\alpha \in [\ell - 4]$, we can define $\eta_\alpha$ that outputs $O(y \log \ell)$ bits and prove that:

$$\left(\tau_{\alpha+1}, h\Big(g\Big(\mathcal{V}_{\alpha+1,\mathsf{ideal}}(\tau_{\alpha+1}), \widehat{\phi}_\alpha(\tau_{\alpha+1})\Big), \eta_{\alpha+1}(\tau_{\alpha+1})\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_\alpha, h\big(\mathcal{V}_{\alpha,\mathsf{ideal}}(\tau_\alpha), \eta_\alpha(\tau_\alpha)\big)\Big) \quad (35)$$

This follows by setting $\beta = \alpha$ in Equation (26) and then applying the sequence of Equations (31, 32, 33) with $(\alpha + 1)$ instead of $(\ell - 2)$.

Our next step will be to replace the left hand side of Equation (35) with

$$\left(\tau_{\alpha+1}, g\Big(h\big(\mathcal{V}_{\alpha+1,\mathsf{ideal}}(\tau_{\alpha+1}), \eta_{\alpha+1}(\tau_{\alpha+1})\big), \widehat{\phi}_\alpha(\tau_{\alpha+1})\Big)\right),$$

i.e., with $h$ and $g$ interchanged. To this end, we prove the following claim about the commutativity of the functions $g$ and $h$.

**Claim 3.** *For any leakage values $\Phi \in \{0, *\}^y$ and $\Pi \in ([-\ell, \ell] \cup *)^y$, and any $\mathcal{X}$,*

$$g(h(\mathcal{X}, \Pi), \Phi) = h(g(\mathcal{X}, \Phi), \Pi). \quad (36)$$

*Proof.* We prove this via the following exhaustive case analysis, for each $i \in [y]$:

- If $\Phi^i = 0$ then $g$ is the identity function, and hence
$$g(h^i(\chi_i, \Pi^i), \Phi^i) = h^i(g(\chi_i, \Phi^i), \Pi^i).$$
- If $\Phi^i = *$ then
$$g(h^i(\chi_i, \Pi^i), \Phi^i) = h^i(g(\chi_i, \Phi^i), \Pi^i) = \bot,$$
where the fact that $g(h^i(\chi_i, \Pi^i), \Phi^i) = \bot$ follows from the fact that $g(\cdot, *) = \bot$, and the fact that $h^i(g(\chi_i, \Phi^i), \Pi^i) = \bot$ follows from the fact that $g(\cdot, *) = \bot$ and the fact that $h^i(\bot, \cdot) = \bot$ (where the latter follows from the definition of $h^i$ together with the fact that $f(\bot, \cdot) = \bot$).

This completes the proof of the claim. □

Therefore, defining $\eta_\ell \equiv 0^y, \eta_{\ell-1} \triangleq \pi_{\ell-1}$, and $\eta_{\ell-2}, \ldots \eta_1$ as defined above, it holds that for every $\alpha \in [\ell-1]$:

$$\left(\tau_{\alpha+1}, g\Big(h\big(\mathcal{V}_{\alpha+1,\mathsf{ideal}}(\tau_{\alpha+1}), \eta_{\alpha+1}(\tau_{\alpha+1})\big), \widehat{\phi}_\alpha(\tau_{\alpha+1})\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_\alpha, h\big(\mathcal{V}_{\alpha,\mathsf{ideal}}(\tau_\alpha), \eta_\alpha(\tau_\alpha)\big)\right) \quad (37)$$

We define $\widehat{\Phi}_1 \triangleq \widehat{\phi}_1$. We would like the right hand side of the equation above for $\alpha$ to be the same as the left hand side applied with $\alpha - 1$, since then could denote the left hand side by $\Big(\tau_{\alpha+1}, J_{\alpha+1}(\tau_{\alpha+1})\Big)$ and the right hand side by $\Big(\tau_\alpha, J_\alpha(\tau_\alpha)\Big)$, we use a standard hybrid argument to argue that

$$\Big(\tau_\ell, J_\ell(\tau_\ell)\Big) \approx \Big(\tau_1, J_1(\tau_1)\Big).$$

In what follows, we modify Equation (37) to have this desired structure.

To this end, substitute $\alpha = 1$ in Equation (37), to obtain

$$\left(\tau_2, g\Big(h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_2), \eta_2(\tau_2)\big), \widehat{\phi}_1(\tau_2)\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_1, h\big(\mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)\big)\right)$$

Similarly, substitute $\alpha = 2$ in Equation (37), to obtain

$$\left(\tau_3, g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\phi}_2(\tau_3)\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_2, h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_2), \eta_2(\tau_2)\big)\right)$$

Set $\widehat{\widehat{\Phi}}_1$ according to the leakage lemma (Lemma 2)[29] such that:

$$\left(\tau_3, g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\phi}_2(\tau_3)\Big), \widehat{\widehat{\Phi}}_1(\tau_3)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_2, h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_2), \eta_2(\tau_2)\big), \widehat{\Phi}_1(\tau_2)\right) \quad (38)$$

Because $g$ is an efficient function,

$$\left(\tau_3, g\Big(g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\phi}_2(\tau_3)\Big), \widehat{\widehat{\Phi}}_1(\tau_3)\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_2, g\Big(h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_2), \eta_2(\tau_2)\big), \widehat{\Phi}_1(\tau_2)\Big)\right) \quad (39)$$

At this point, we will define $\widehat{\Phi}_2(\cdot)$ so that for every $\tau$ and every $i \in [y]$,

$$(\widehat{\Phi}_2^i(\tau) = *) \text{ if } (\widehat{\phi}_2^i(\tau) = * \text{ or } \widehat{\widehat{\Phi}^i}_1(\tau) = *), \text{ and } 0 \text{ otherwise.}$$

Note that

$$g\Big(g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\phi}_2(\tau_3)\Big), \widehat{\widehat{\Phi}}_1(\tau_3)\Big) = g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\Phi}_2(\tau_3)\Big)$$

Substituting this in Equation (39),

$$\left(\tau_3, g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\Phi}_2(\tau_3)\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_2, g\Big(h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_2), \eta_2(\tau_2)\big), \widehat{\Phi}_1(\tau_2)\Big)\right)$$

[29] This is the third sequential application of the leakage lemma.

Similarly, starting with Equation (37) and applying Lemma 2, we can define $\widehat{\Phi}_3$ such that:

$$\Big(\tau_4, g\Big(h\big(\mathcal{V}_{4,\mathsf{ideal}}(\tau_4), \eta_4(\tau_4)\big), \widehat{\Phi}_3(\tau_4)\Big)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_3, g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\Phi}_2(\tau_3)\Big)\Big) \tag{40}$$

This follows by substituting $\alpha = 3$ in Equation (37), and then applying Equations (38) and (39), with 3 instead of 2, and relying on $\widehat{\Phi}_2$ instead of $\widehat{\Phi}_1$.

Similarly, we define $\widehat{\Phi}_4, \cdots \widehat{\Phi}_{\ell-1}$. Setting

$$J_1(\tau_1) = h(\mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)),$$

and

$$J_\alpha(\tau_\alpha) = g\Big(h\big(\mathcal{V}_{\alpha,\mathsf{ideal}}(\tau_\alpha), \eta_\alpha(\tau_\alpha)\big), \widehat{\Phi}_{\alpha-1}(\tau_\alpha)\Big) \text{ for } \alpha \in [2, \ell],$$

we conclude that for all $\alpha \in [2, \ell]$:

$$\big(\tau_\alpha, J_\alpha(\tau_\alpha)\big) \approx \big(\tau_{\alpha-1}, J_{\alpha-1}(\tau_{\alpha-1})\big).$$

This follows by starting with Equation (37), and then applying Equations (38) and (39), with $\alpha$ instead of 3.

This implies

$$\Big(\tau_1, J_1(\tau_1)\big) \approx \big(\tau_\ell, J_\ell(\tau_\ell)\Big)$$

Recall that by Lemma 1 we have,

$$\Big(\tau_1, \mathcal{V}_{1,\mathsf{ideal}}(\tau_1)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_0, \mathcal{V}_{1,\mathsf{real}}(\tau_0)\Big) \tag{41}$$

We set $\widehat{\eta}_1$ according to the leakage lemma (Lemma 2) such that:

$$\Big(\tau_1, \mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_0, \mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)$$

This, together with the fact that $h$ is efficiently computable, implies that

$$\Big(\tau_1, h\Big(\mathcal{V}_{1,\mathsf{ideal}}(\tau_1), \eta_1(\tau_1)\Big)\Big) \approx_{\mathsf{poly}(n\cdot 2^y)} \Big(\tau_0, h\Big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)\Big)$$

Define $J_0(\tau_0) = h\Big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)$, then we have that for all $\alpha \in [1, \ell]$,

$$\big(\tau_\alpha, J_\alpha(\tau_\alpha)\big) \approx \big(\tau_{\alpha-1}, J_{\alpha-1}(\tau_{\alpha-1})\big) \tag{42}$$

We define $F$ as a function that on input a tuple $(\chi_1, \ldots, \chi_y)$ outputs $(\widetilde{m}_1, \ldots, \widetilde{m}_y)$ such that for all $i \in [y]$, if $\chi_i = (\widetilde{M}, \psi)$ for some $\widetilde{M} \in \{0,1\}^p$ and some $\psi \geq 0$, then $\widetilde{m}_i = \widetilde{M}$, else $\widetilde{m}_i = \perp$. We then define $\mathcal{V}_{\mathsf{Real}}$ as

$$\mathcal{V}_{\mathsf{Real}}(\tau_0) = F\Big(J_0(\tau_0)\Big) = F\Big(h\Big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)\Big)$$

and $\mathcal{V}_{\mathsf{Ideal}}$ as

$$\mathcal{V}_{\mathsf{Ideal}}(\tau_\ell) = F\Big(J_\ell(\tau_\ell)\Big) = F\Big(g(\mathcal{V}_{\ell,\mathsf{ideal}}, \widehat{\Phi}_{\ell-1}(\tau_\ell))\Big)$$

which by Equation (42), implies that

$$\Big(\tau_0, \mathcal{V}_{\mathsf{Real}}(\tau_0)\Big) \approx \Big(\tau_\ell, \mathcal{V}_{\mathsf{Ideal}}(\tau_\ell)\Big)$$

**Efficiency of computing $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$.** Note that $\mathcal{V}_{\mathsf{Real}}(\tau_0) = F\Big(h\Big(\mathcal{V}_{1,\mathsf{real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)\Big)$, where $F$ and $h$ are efficiently computable, and $\mathcal{V}_{1,\mathsf{real}}$ is computable in time $T_V$. Moreover, $\widehat{\eta}_1$ outputs a string of length at most $O(y \log \ell)$, and is defined as the result of applying the leakage lemma (Lemma 2) to Equation (41). Therefore, setting $\gamma = O(y \log \ell)$ and $T = n \cdot 2^y$ in Lemma 2, the function $\widehat{\eta}_1$ is computable in time $(n \cdot 2^y)^{O(\log n)}$.

Similarly, $\mathcal{V}_{\mathsf{Ideal}}(\tau_\ell) = F\Big(g(\mathcal{V}_{\ell,\mathsf{ideal}}, \widehat{\Phi}_{\ell-1}(\tau_\ell))\Big)$, where $F$ and $g$ are efficiently computable, and $\mathcal{V}_{\ell,\mathsf{ideal}}$ is computable in time $T_V$. We next argue that $\widehat{\Phi}_{\ell-1}$ is computable in time $(n \cdot 2^y)^{O(\log n)}$. To this end, recall that $\Phi_{\ell-1} = \widehat{\phi}_{\ell-1} + \widehat{\widehat{\Phi}}_{\ell-2}$, and thus it suffices to bound the running time of $\widehat{\phi}_{\ell-1}$ and $\widehat{\widehat{\Phi}}_{\ell-2}$. Recall that $\widehat{\phi}_{\ell-1}$ outputs a string of length $O(\log y)$, and is defined as the result of applying the leakage lemma (Lemma 2) to Equation (37). Therefore, setting $\gamma = O(y)$ and $T = n \cdot 2^y$ the function $\widehat{\phi}_{\ell-1}$ is computable in time $(n \cdot 2^y)^{O(\log n)}$. Similarly, $\widehat{\widehat{\Phi}}_{\ell-2}$ outputs a string of length $O(\log y)$, and is again defined as the result of applying the leakage lemma (Lemma 2). Therefore, setting $\gamma = O(y)$ and $T = n \cdot 2^y$ in Lemma 2, the function $\widehat{\widehat{\Phi}}_{\ell-1}$ is computable in time $(n \cdot 2^y)^{O(\log n)}$. Therefore, $\widehat{\Phi}_{\ell-1}$ is computable in time $(n \cdot 2^y)^{O(\log n)}$.

We thus conclude that $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ are computable in time $T'_V = T_V + (n \cdot 2^y)^{O(\log n)}$, as desired.

**Validity of $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$.** We now prove that $\mathcal{V}_{\mathsf{Real}}$ and $\mathcal{V}_{\mathsf{Ideal}}$ satisfy the validity condition in Definition 3.

**Proving that $\mathcal{V}_{\mathsf{Real}}$ satisfies the validity condition.**

Recall that $\mathcal{V}_{\mathsf{Real}}(\tau_0) = F\Big(h\Big(\mathcal{V}_{1,\mathsf{Real}}(\tau_0), \widehat{\eta}_1(\tau_0)\Big)\Big)$. First, we note that for every $\beta \in [\ell]$, $\mathcal{V}_{\beta,\mathsf{Real}}$ and $\mathcal{V}_{\beta,\mathsf{Ideal}}$ invoke $v_{\mathsf{Real}}$ or $v_{\mathsf{Ideal}}$ respectively on the underlying commitments corresponding to adversary's small tags $\widetilde{\lambda}_\beta$ in all the right sessions. Therefore by construction, for every $\beta \in [\ell]$ and every $i \in [y]$, and for every transcript $\tau$ in which the $i^{th}$ commitment $\widetilde{c}_i$ is valid (i.e., is of the form $\widetilde{c}_i = \mathsf{com}(\widetilde{M}; r)$ for some $\widetilde{M}$ and $r$), it holds that $\mathcal{V}^i_{\beta,\mathsf{Real}}(\tau)$ outputs $(\widetilde{M}, k)$. Hence, to prove that $\mathcal{V}_{\mathsf{Real}}$ satisfies the validity condition, it suffices to prove that for every $i \in [y]$,

$$\Pr\left[\left(\mathcal{V}^i_{1,\mathsf{Real}}(\tau_0) = (\widetilde{M}, k)\right) \wedge \left(\widehat{\eta}^i_1(\tau_0) = *\right)\right] = \mathsf{negl}(n)$$

We prove the following stronger equation, for every $i \in [y]$:

$$\Pr\left[\left(\mathcal{V}^i_{1,\mathsf{Real}}(\tau_0) \neq \bot\right) \wedge \left(\widehat{\eta}^i_1(\tau_0) = *\right)\right] = \mathsf{negl}(n)$$

Recall that for any $\beta \in [\ell - 1]$, by definition of $\pi_\beta$, for all $i \in [y]$,

$$\pi^i_\beta(\tau_\beta) = * \implies \mathcal{V}^i_{\beta,\mathsf{Ideal}}(\tau_\beta) = \bot. \tag{43}$$

Setting $\beta = [\ell - 1]$ in Equation (43), for all $i \in [y]$, $\pi^i_{\ell-1}(\tau_{\ell-1}) = * \implies \mathcal{V}^i_{\ell-1,\mathsf{Ideal}}(\tau_{\ell-1}) = \bot$.

Recall that $\eta_{\ell-1} \triangleq \pi_{\ell-1}$. Since $\widehat{\eta}_{\ell-1}$ is computed based on $\eta_{\ell-1}$ by applying the leakage lemma (refer to Equation (12)), we have that for all $i \in [y]$,

$$\Pr\Big[\left(f^i(\mathcal{V}^i_{\ell-2,\mathsf{Ideal}}(\tau_{\ell-2}), \pi^i_{\ell-2}(\tau_{\ell-2})\right) \neq \bot) \wedge \left(\widehat{\eta}^i_{\ell-1}(\tau_{\ell-2}) = *\right)\Big] = \mathsf{negl}(n).$$

Next, we prove that for every $\beta$, there exists a negligible function $\mu_\beta$, such that for every $\beta \in [\ell-3]$, if

$$\Pr\Big[\big(f^i\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1}),\pi^i_\beta(\tau_{\beta+1})\big)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+2}(\tau_{\beta+1})=*\big)\Big]=\epsilon$$

then

$$\Pr\Big[\big(f^i\big(\mathcal{V}^i_{\beta,\mathsf{Ideal}}(\tau_{\beta}),\pi^i_\beta(\tau_{\beta})\big)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+1}(\tau_{\beta})=*\big)\Big]\leq\epsilon+\mu_\beta(n).$$

Fix any $\beta \in [\ell-3]$. By definition, $\eta^i_{\beta+1}(\tau)=* \iff (\widehat{\eta}^i_{\beta+2}(\tau)=*)$ or $(\pi^i_{\beta+1}(\tau)=*)$. Therefore,

$$\begin{aligned}
&\Pr\Big[\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1})\neq\perp\big)\ \wedge\ \big(\eta^i_{\beta+1}(\tau_{\beta+1})=*\big)\Big]\\
&=\Pr\Big[\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1})\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+2}(\tau_{\beta+1})=*\big)\ \wedge\ \big(\pi^i_{\beta+1}(\tau_{\beta+1})\neq*\big)\Big]\\
&+\Pr\Big[\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1})\neq\perp\big)\ \wedge\ \big(\pi^i_{\beta+1}(\tau_{\beta+1})=*\big)\Big]\\
&=\Pr\Big[\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1})\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+2}(\tau_{\beta+1})=*\big)\ \wedge\ \big(\pi^i_{\beta+1}(\tau_{\beta+1})\neq*\big)\Big]+0\\
&=\Pr\Big[f^i\big(\mathcal{V}^i_{\beta+1,\mathsf{Ideal}}(\tau_{\beta+1}),\pi^i_{\beta+1}(\tau_{\beta+1})\big)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+2}(\tau_{\beta+1})=*\big)\ \wedge\ \big(\pi^i_{\beta+1}(\tau_{\beta+1})\neq*\big)\Big]\quad=\epsilon
\end{aligned}$$

Since $\widehat{\eta}_{\beta+1}$ is computed based on $\eta_{\beta+1}$ by applying the leakage lemma to Equation (9) (w.r.t. $\beta+1$), we have that for all $i \in [y]$,

$$\Pr\Big[\big(f^i\big(\mathcal{V}^i_{\beta,\mathsf{Ideal}}(\tau_{\beta}),\pi^i_\beta(\tau_{\beta})\big)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+1}(\tau_{\beta})=*\big)\Big]\leq\epsilon+\mu_\beta(n),$$

for some negligible function $\mu_\beta$, as required. This implies that for every $\beta \in [1,\ell-3]$,

$$\Pr\Big[\big(f^i\big(\mathcal{V}^i_{\beta,\mathsf{Ideal}}(\tau_{\beta}),\pi^i_\beta(\tau_{\beta})\big)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_{\beta+1}(\tau_{\beta})=*\big)\Big]=\mathsf{negl}(n)$$

Specifically, setting $\beta=1$, we have that for every $i \in [y]$,

$$\Pr\Big[f^i\big(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1)\pi^i_1(\tau_1)\big)\neq\perp\ \wedge\ \big(\widehat{\eta}^i_2(\tau_1)=*\big)\Big]=\mathsf{negl}(n)$$

Since by definition, $\eta^i_1(\tau)=* \iff (\widehat{\eta}^i_2(\tau)=*)$ or $(\pi^i_1(\tau)=*)$, this implies:

$$\begin{aligned}
&\Pr\Big[\big(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1)\neq\perp\big)\ \wedge\ \big(\eta^i_1(\tau_1)=*\big)\Big]\\
&=\Pr\Big[\big(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_2(\tau_1)=*\big)\ \wedge\ \big(\pi^i_1(\tau_1)\neq*\big)\Big]+\Pr\Big[\big(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1)\neq\perp\big)\ \wedge\ \big(\pi^i_1(\tau_1)=*\big)\Big]\\
&=\Pr\Big[\big(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_2(\tau_1)=*\big)\ \wedge\ \big(\pi^i_1(\tau_1)\neq*\big)\Big]+0\\
&=\Pr\Big[\big(f(\mathcal{V}^i_{1,\mathsf{Ideal}}(\tau_1),\pi^i_1(\tau_1))\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_2(\tau_1)=*\big)\ \wedge\ \big(\pi^i_1(\tau_1)\neq*\big)\Big]+0\\
&=\mathsf{negl}(n)
\end{aligned}$$

Since $\widehat{\eta}_1$ is derived from $\eta_1$ by applying the leakage lemma to Equation (41), we have that for every $i \in [y]$,

$$\Pr\Big[\big(\mathcal{V}^i_{1,\mathsf{Real}}(\tau_0)\neq\perp\big)\ \wedge\ \big(\widehat{\eta}^i_1(\tau_0)=*\big)\Big]=\mathsf{negl}(n),$$

as desired.

**Proving that $\mathcal{V}_{\mathsf{Ideal}}$ satisfies the validity condition.**

Recall that $\mathcal{V}_{\mathsf{Ideal}}(\tau_\ell) = F\Big(g\Big(\mathcal{V}_{\ell,\mathsf{Ideal}}(\tau_\ell), \widehat{\Phi}_{\ell-1}(\tau_\ell)\Big)\Big)$. First, we note that for every $\beta \in [\ell]$, $\mathcal{V}_{\beta,\mathsf{Real}}$ and $\mathcal{V}_{\beta,\mathsf{Ideal}}$ invoke $v_{\mathsf{Real}}$ or $v_{\mathsf{Ideal}}$ respectively on the underlying commitments corresponding to adversary's small tags $\widetilde{\lambda}_\beta$ in all the right sessions. Therefore by construction, for every $\beta \in [\ell]$ and every $i \in [y]$, and for every transcript $\tau$ in which the $i^{th}$ commitment $\widetilde{c}_i$ is valid (i.e., is of the form $\widetilde{c}_i = \mathsf{com}(\widetilde{M}; r)$ for some $\widetilde{M}$ and $r$), it holds that $\mathcal{V}^i_{\beta,\mathsf{Ideal}}(\tau)$ outputs $(\widetilde{M}, k)$. Hence, to prove that $\mathcal{V}_{\mathsf{Ideal}}$ satisfies the validity condition, it suffices to prove that for every $i \in [y]$,

$$\Pr\Big[\big(\mathcal{V}^i_{\ell,\mathsf{Ideal}}(\tau_\ell) \in \{(\widetilde{M}, k)\}_{\widetilde{M}\in\{0,1\}^p}\big) \ \wedge \ \big(\widehat{\Phi}^i_{\ell-1}(\tau_\ell) = *\big)\Big] = \mathsf{negl}(n).$$

First, we recall that for every $\beta \in [\ell-1]$ and every $i \in [y]$, by definition

$$(\phi^i_\beta(\tau_\beta) = *) \iff (\pi^i_\beta(\tau_\beta) = *)$$

Moreover, if $(\pi^i_\beta(\tau_\beta) = *)$ then

$$\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau_\beta) = \left(\widetilde{M}, \frac{3k}{4} - \beta + b\right) \text{ for some } \widetilde{M} \in \{0,1\}^p, b \in \{0,1\}.$$

Therefore, if $(\phi^i_\beta(\tau_\beta) = *)$ then

$$\mathcal{V}^i_{\beta+1,\mathsf{real}}(\tau_\beta) = \left(\widetilde{M}, \frac{3k}{4} - \beta + b\right) \text{ for some } \widetilde{M} \in \{0,1\}^p, b \in \{0,1\}.$$

Recall that for $\beta \in [\ell-1]$, by Equation (25),

$$\big(\tau_{\beta+1}, \mathcal{V}_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \widehat{\phi}_\beta(\tau_{\beta+1})\big) \approx \big(\tau_\beta, \mathcal{V}_{\beta+1,\mathsf{real}}(\tau_\beta), \phi_\beta(\tau_\beta)\big).$$

Therefore for every $\beta \in [\ell-1]$ and every $i \in [y]$,

$$\Pr\Big[\big(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}) \notin \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi\in\left\{\frac{3k}{4}-\beta, \frac{3k}{4}-\beta+1\right\}}\big) \ \wedge \ \big(\widehat{\phi}^i_\beta(\tau_{\beta+1}) = *\big)\Big] = \mathsf{negl}(n). \quad (44)$$

Recall that for every $i \in [y]$, $h^i$ on input $((\widetilde{M}, \psi), \alpha)$, for every $\alpha$ in the range of $\eta^i_{\beta+1}(\cdot)$ outputs either $\perp$ (if $\alpha = *$) or $(\widetilde{M}, \psi')$, where $\psi' \in [\psi - \ell + \beta + 1, \psi + \ell - \beta - 1]$[30]. Therefore, if

$$\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}) \in \left\{\left(\widetilde{M}, \frac{3k}{4} - \beta\right), \left(\widetilde{M}, \frac{3k}{4} - \beta + 1\right)\right\}$$

then

$$h^i\left(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \eta^i_{\beta+1}(\tau_{\beta+1})\right) = * \text{ or,}$$

$$h^i\left(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \eta^i_{\beta+1}(\tau_{\beta+1})\right) = (\widetilde{M}, \psi') \text{ where } \psi' \in \left[\frac{3k}{4} - \ell + 1, \frac{3k}{4} + \ell\right]$$

which implies that for every $i \in [y], \beta \in [\ell-1]$, there exists a negligible function $\mu$ such that

$$\Pr\left[\left(h^i\left(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \eta^i_{\beta+1}(\tau_{\beta+1})\right) \notin \{*\}\cup\{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi\in\left\{\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right\}}\right) \wedge \left(\widehat{\phi}^i_\beta(\tau_{\beta+1}) = *\right)\right] = \mu(n). \quad (45)$$

[30] This is because $\eta^i_{\beta+1}$ outputs values in the range $[-\ell + (\beta+1), \ell - (\beta+1)]$.

Recall that by Equation (37), for all $\beta \in [\ell - 1]$:

$$\left(\tau_{\beta+1}, g\Big(h\big(\mathcal{V}_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \eta_{\beta+1}(\tau_{\beta+1})\big), \widehat{\phi}_\beta(\tau_{\beta+1})\Big)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\tau_\beta, h\big(\mathcal{V}_{\beta,\mathsf{ideal}}(\tau_\beta), \eta_\beta(\tau_\beta)\big)\right)$$

Therefore taking $\beta = 2$ and applying the leakage lemma, we get that $\widehat{\widehat{\Phi}}_1 \triangleq \widehat{\widehat{\phi}}_1$ is such that:

$$\left(\left(\tau_3, g\Big(h\big(\mathcal{V}_{3,\mathsf{ideal}}(\tau_3), \eta_3(\tau_3)\big), \widehat{\phi}_2(\tau_3)\Big)\right), \widehat{\widehat{\phi}}_1(\tau_3)\right) \approx_{\mathsf{poly}(n\cdot 2^y)} \left(\left(\tau_2, h\big(\mathcal{V}_{2,\mathsf{ideal}}(\tau_\beta), \eta_2(\tau_2)\big)\right), \widehat{\phi}_1(\tau_2)\right)$$

Combining this with Equation (45), we have that for every $i \in [y]$,

$$\Pr\left[\left(g\Big(h^i\big(\mathcal{V}^i_{3,\mathsf{ideal}}(\tau_3), \eta^i_3(\tau_3)\big), \widehat{\phi}^i_2(\tau_3)\Big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left[\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right]}\right) \wedge \left(\widehat{\widehat{\Phi}}^i_1(\tau_3) = *\right)\right] = \mathsf{negl}(n)$$

Next, we prove that for every $\beta \in [3, \ell - 1]$ there exists a negligible function $\mu_\beta$ such that if:

$$\Pr\left[\left(g\Big(h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big), \widehat{\phi}^i_{\beta-1}(\tau_\beta)\Big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left[\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right]}\right) \wedge \left(\widehat{\widehat{\Phi}}^i_{\beta-2}(\tau_\beta) = *\right)\right] = \varepsilon$$

then

$$\Pr\Bigg[\left(g\Big(h^i\big(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}), \eta^i_{\beta+1}(\tau_{\beta+1})\big), \widehat{\phi}^i_\beta(\tau_{\beta+1})\Big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left[\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right]}\right)$$
$$\wedge \left(\widehat{\widehat{\Phi}}^i_{\beta-1}(\tau_{\beta+1}) = *\right)\Bigg] \leq \varepsilon + \mu_\beta(n)$$

To this end, fix any $\beta \in [3, \ell - 1]$.

Since $\widehat{\Phi}^i_{\beta-1}(\tau) = * \iff (\widehat{\phi}^i_{\beta-1} = * \text{ OR } \widehat{\widehat{\Phi}}^i_{\beta-2} = *)$, we have for every $i \in [y]$,

$$\Pr\left[\left(h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left\{\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right\}}\right) \wedge \left(\widehat{\Phi}^i_{\beta-1}(\tau_\beta) = *\right)\right]$$
$$= \Pr\left[h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left\{\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right\}} \wedge \left(\widehat{\phi}^i_{\beta-1}(\tau_\beta) = *\right)\right]$$
$$+ \Pr\left[h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left\{\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right\}} \wedge \left(\widehat{\widehat{\Phi}}^i_{\beta-2}(\tau_\beta) = *\right) \wedge \left(\widehat{\phi}^i_{\beta-1}(\tau_\beta) \neq *\right)\right]$$
$$= \Pr\left[h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left\{\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right\}} \wedge \left(\widehat{\phi}^i_{\beta-1}(\tau_\beta) = *\right)\right]$$
$$+ \Pr\Bigg[g\Big(h^i\big(\mathcal{V}^i_{\beta,\mathsf{ideal}}(\tau_\beta), \eta^i_\beta(\tau_\beta)\big), \widehat{\phi}^i_{\beta-1}(\tau_\beta)\Big) \notin \{*\} \cup \{(\widetilde{M}, \psi)\}_{\widetilde{M}\in\{0,1\}^p, \psi \in \left[\frac{3k}{4}-\ell+1, \frac{3k}{4}+\ell\right]} \wedge \left(\widehat{\widehat{\Phi}}^i_{\beta-2}(\tau_\beta) = *\right)$$
$$\wedge \left(\widehat{\phi}^i_{\beta-1}(\tau_\beta) \neq *\right)\Bigg]$$
$$\leq \mu(n) + \varepsilon.$$

Since $\widehat{\widehat{\Phi}}_{\beta-1}$ is obtained by applying the leakage lemma (Lemma 2) to Equation (37), we have that for every $i \in [y]$, there exists a negligible function $\mu'_\beta$ such that

$$\Pr\Bigg[\Big(g\Big(h^i\big(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}),\eta^i_{\beta+1}(\tau_{\beta+1})\big),\widehat{\phi}^i_\beta(\tau_{\beta+1})\Big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge$$

$$\Big(\widehat{\widehat{\Phi}}^i_{\beta-1}(\tau_{\beta+1})=*\Big)\Bigg] \le \varepsilon+\mu(n)+\mu'_\beta(n)$$

Setting $\mu_\beta = \mu+\mu'_\beta$, we have

$$\Pr\Bigg[\Big(g\Big(h^i\big(\mathcal{V}^i_{\beta+1,\mathsf{ideal}}(\tau_{\beta+1}),\eta^i_{\beta+1}(\tau_{\beta+1})\big),\widehat{\phi}^i_\beta(\tau_{\beta+1})\Big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge$$

$$\Big(\widehat{\widehat{\Phi}}^i_{\beta-1}(\tau_{\beta+1})=*\Big)\Bigg] \le \varepsilon+\mu_\beta(n)$$

as desired.

This implies that (setting $\beta=\ell-1$):

$$\Pr\Bigg[g\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big),\widehat{\phi}^i_{\ell-1}(\tau_\ell)\Big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\widehat{\Phi}}^i_{\ell-2}(\tau_\ell)=*\Big)\Bigg] = \mathsf{negl}(n).$$

Since $\widehat{\Phi}^i_{\ell-1}(\tau)=* \iff (\widehat{\phi}^i_{\ell-1}=* \text{ OR } \widehat{\widehat{\Phi}}^i_{\ell-2}=*)$, we have for every $i\in[y]$,

$$\begin{aligned}
&\Pr\Bigg[\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\Phi}^i_{\ell-1}(\tau_\ell)=*\Big)\Bigg]\\
&= \Pr\Bigg[\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\phi}^i_{\ell-1}(\tau_\ell)=*\Big)\Bigg]\\
&+ \Pr\Bigg[\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\widehat{\Phi}}^i_{\ell-2}(\tau_\beta)=*\Big) \wedge \Big(\widehat{\phi}^i_{\ell-1}(\tau_\ell)\neq *\Big)\Bigg]\\
&= \Pr\Bigg[\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\phi}^i_{\ell-1}(\tau_\ell)=*\Big)\Bigg]\\
&+ \Pr\Bigg[g\Big(h^i\big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell),\eta^i_\ell(\tau_\ell)\big),\widehat{\phi}^i_{\ell-1}(\tau_\ell)\Big) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell+1,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\widehat{\Phi}}^i_{\ell-2}(\tau_\beta)=*\Big)\\
&\wedge \Big(\widehat{\phi}^i_{\ell-1}(\tau_\ell)\neq *\Big)\Bigg]\\
&= \mu(n)+\mathsf{negl}(n) = \mathsf{negl}(n).
\end{aligned}$$

Since $\eta_\ell := 0^y$, this implies:

$$\Pr\Bigg[\Big(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell) \notin \{*\}\cup\{(\widetilde{M},\psi)\}_{\widetilde{M}\in\{0,1\}^p,\psi\in\left[\frac{3k}{4}-\ell,\frac{3k}{4}+\ell\right]}\Big) \wedge \Big(\widehat{\Phi}^i_{\ell-1}(\tau_\ell)=*\Big)\Bigg] = \mathsf{negl}(n)$$

which implies

$$\Pr\left[\left(\mathcal{V}^i_{\ell,\mathsf{ideal}}(\tau_\ell) \notin \{(\widetilde{M},k)\}_{\widetilde{M}\in\{0,1\}^p}\right) \wedge \left(\widehat{\Phi}^i_{\ell-1}(\tau_\ell) = *\right)\right] = \mathsf{negl}(n),$$

as desired. This completes the proof of validity, and also concludes the proof of the theorem. □

# 6 Putting Things Together: Non-Malleable Commitments for All Tags

In this section, we describe how one can combine results from Section 4 and Section 5 to obtain our main result.

**Theorem 3.** *There exists a non-interactive non-malleable commitment w.r.t. replacement satisfying Definition 1, assuming the following:*

- Sub-exponential hardness of factoring or discrete log.
- Sub-exponential quantum hardness of LWE.
- Sub-exponential non-interactive witness indistinguishable (NIWI) proofs.

*Proof.* To obtain this theorem, we apply the following sequence of steps:

- Let $\mathcal{C}_{[\eta \log\log n]}$ denote a many-to-many same-tag non-malleable commitment w.r.t. commitment satisfying Definition 4, for $\eta \log\log n$ tags where $0 < \eta < 1$, secure against $2^{\mathsf{poly}\log n}$-size adversaries. Such a scheme is constructed in Theorem 1, assuming sub-exponential hardness of factoring or discrete log, and sub-exponential quantum hardness of LWE. By Remark 2, this scheme also satisfies Definition 3 for any polynomials $\ell$ and $y$.

- Apply the compiler in Section 5 to $\mathcal{C}_{[\eta \log\log n]}$.

  Specifically, setting $y = \log^3 n, \ell = \log^3 n, z = \log^7 n, t = \eta \log\log n$ in Theorem 2, we note that $z \geq 10\ell y$ and $\mathcal{C}_{[\eta \log\log n]}$ is $5\ell t$-to-$z$ same-tag auxiliary-input non-malleable w.r.t. replacement against $\mathsf{poly}(n \cdot 2^y)$-size adversaries.

  Therefore, Theorem 2 gives a $(\log^3 n)$-to-$(\log^3 n)$ same-tag auxiliary-input non-malleable commitment w.r.t. replacement satisfying Definition 3, for $\log^\epsilon n$ tags, (for a small constant $\epsilon > 0$), against polynomial-size adversaries.

  Denote this resulting scheme by $\mathcal{C}_{[\log^\epsilon n]}$.

- Apply the compiler in Section 5 once again, this time to $\mathcal{C}_{[\log^\epsilon n]}$.

  Specifically, setting $y = 10, \ell = 10\log^2 n, z = 1000\log^2 n, t = \log^\epsilon n$ in Theorem 2, we note that $z = 10\ell y$ and that $\mathcal{C}_{[\log^\epsilon n]}$ is $5\ell t$-to-$z$ same-tag auxiliary-input non-malleable w.r.t. replacement against $\mathsf{poly}(n \cdot 2^y)$-size adversaries.

  Therefore, Theorem 2 gives a $10\log^2 n$-to-10 same-tag auxiliary-input non-malleable commitment w.r.t. replacement satisfying Definition 3, for $2\log^2 n$ tags, against polynomial-size adversaries.

  Denote this resulting scheme by $\mathcal{C}_{[2\log^2 n]}$.

- Apply the compiler in Section 5 one final time, this time to To $\mathcal{C}_{[2\log^2 n]}$.

  Specifically, setting $\ell = y = 1, z = 10, t = 2\log^2 n$ in Theorem 2, we note that $z = 10\ell y$ and that $\mathcal{C}_{[\log^2 n]}$ is $5\ell t$-to-$z$ same-tag auxiliary-input non-malleable w.r.t. replacement against $\mathsf{poly}(n \cdot 2^y)$-size adversaries.

  Therefore, Theorem 2 gives a a 1-to-1 auxiliary-input non-malleable commitment w.r.t. replacement satisfying Definition 3, for $n^{\log n}$ tags, against polynomial-size adversaries. Denote this resulting scheme by $\mathcal{C}_{[n^{\log n}]}$.

- Next, assume the existence of a sub-exponentially secure digital signature scheme. More specifically, assume the existence of a signature scheme such that poly-size adversary cannot forge signatures w.r.t. verification keys of size $\log^2 n$ (except with negligible probability). Such a scheme is implied by sub-exponential one-way functions. Denote the keys for such a scheme by $(vk, sk)$, the setup algorithm by $\mathsf{Setup}(1^\lambda)$ and the signing algorithm by $\mathsf{Sign}(sk, \cdot)$.

  Then starting with a non-malleable commitment scheme (w.r.t. replacement) according to Definition 1 for tags in $[n^{\log n}]$ (denoted by $\mathcal{C}_{[n^{\log n}]}$), we build non-malleable commitments for tags in $[2^n]$, satisfying Definition 1 as follows:

  To commit to message $m$ with tag $T \in [2^n]$, sample $(vk, sk) \xleftarrow{\$} \mathsf{Setup}(1^{\log^2 n})$, compute a commitment $c \leftarrow \mathsf{Com}_{vk}(m)$, and a signature $\sigma \leftarrow \mathsf{Sign}(sk, T)$. Output $(vk, c, \sigma)$. Here $\mathsf{Com}_{vk}(\cdot)$ denotes the (randomized) commitment algorithm of $\mathcal{C}_{[n^{\log n}]}$ corresponding to tag $vk$, and we note that $|vk| = \log^2 n$ bits.

  For every PPT man-in-the-middle $\mathcal{A}$ that outputs $(\widetilde{vk}, \widetilde{c}, \widetilde{\sigma})$, one of the following holds.

  - Either $\widetilde{vk} = vk$, in which case by unforgeability of the signature scheme, if $\widetilde{T} \neq T$ then $\widetilde{\sigma}$ does not verify.
  - Or $\widetilde{vk} \neq vk$, in which case the message committed to in $\widetilde{c}$ is "unrelated" to the message committed to in $c$, i.e., it satisfies the non-malleability condition of Definition 1, since we assume that $\mathsf{Com}_{vk}$ satisfies Definition 1.

□

## References


[Bar02] Boaz Barak. Constant-Round Coin-Tossing with a Man in the Middle or Realizing the Shared Random String Model. In *FOCS 2002*, pages 345–355, 2002. 1

[BD18] Zvika Brakerski and Nico Döttling. Two-message statistically sender-private OT from LWE. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 370–390. Springer, 2018. 52, 53

[BDK+18] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Huijia Lin, and Tal Malkin. Non-malleable codes against bounded polynomial time tampering. *IACR Cryptology ePrint Archive*, 2018:1015, 2018. 6

[BFMR18] Brandon Broadnax, Valerie Fetzer, Jörn Müller-Quade, and Andy Rupp. Non-malleability vs. cca-security: The case of commitments. In Michel Abdalla and Ricardo Dahab, editors, *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II*, volume 10770 of *Lecture Notes in Computer Science*, pages 312–337. Springer, 2018. 2, 3, 5

[BGI+17] Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia. Two-message witness indistinguishability and secure computation in the plain model from new assumptions. *IACR Cryptology ePrint Archive*, 2017:433, 2017. 52, 53, 54

[BL18] Nir Bitansky and Huijia Lin. One-message zero knowledge and non-malleable commitments. *IACR Cryptology ePrint Archive*, 2018:613, 2018. 1, 4, 6

[BOV07] Boaz Barak, Shien Jin Ong, and Salil P. Vadhan. Derandomization in cryptography. *SIAM J. Comput.*, 37(2):380–400, 2007. 4, 32

[BP04] Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In *CRPTO 2004*, pages 273–289, 2004. 5

[BP15] Nir Bitansky and Omer Paneth. Zaps and non-interactive witness indistinguishability from indistinguishability obfuscation. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part II*, volume 9015 of *Lecture Notes in Computer Science*, pages 401–427. Springer, 2015. 4

[CGM+16] Nishanth Chandran, Vipul Goyal, Pratyay Mukherjee, Omkant Pandey, and Jalaj Upadhyay. Block-wise non-malleable codes. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 31:1–31:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. 5

[CLP15] Kai-Min Chung, Edward Lui, and Rafael Pass. From weak to strong zero-knowledge and applications. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 66–92. Springer, 2015. 32

[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, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 270–299. Springer, 2016. 1, 5

[COSV17] Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Four-round concurrent non-malleable commitments from one-way functions. In *Annual International Cryptology Conference*, pages 127–157. Springer, 2017. 1

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-Malleable Cryptography (Extended Abstract). In *STOC 1991*, 1991. 1, 6

[FF18] Peter Fenteany and Benjamin Fuller. Non-malleable digital lockers. Cryptology ePrint Archive, Report 2018/957, 2018. https://eprint.iacr.org/2018/957. 6

[GHKW17] Rishab Goyal, Susan Hohenberger, Venkata Koppula, and Brent Waters. A generic approach to constructing and proving verifiable random functions. In Kalai and Reyzin [KR17], pages 537–566. 3, 23, 24

[GKS16] Vipul Goyal, Dakshita Khurana, and Amit Sahai. Breaking the three round barrier for non-malleable commitments. In *FOCS*, 2016. 2, 5

[GLOV12] Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, and Ivan Visconti. Constructing non-malleable commitments: A black-box approach. In *FOCS*, 2012. 1

[GOS12] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *J. ACM*, 59(3):11:1–11:35, 2012. 4, 32

[Goy11] Vipul Goyal. Constant Round Non-malleable Protocols Using One-way Functions. In *STOC 2011*, pages 695–704. ACM, 2011. 1, 2, 6, 13

[GPR16] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In *STOC*, pages 1128–1141, New York, NY, USA, 2016. ACM. 1

[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. In *FOCS 2014*, pages 41–50, 2014. 1, 5

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In Lance Fortnow and Salil P. Vadhan, editors, *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, pages 99–108. ACM, 2011. 3, 4, 9, 11, 31, 32

[JKKR17] Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Ron Rothblum. Distinguisher-dependent simulation in two rounds and its applications. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 158–189. Springer, 2017. 4, 52, 53, 54

[JP14] Dimitar Jetchev and Krzysztof Pietrzak. How to fake auxiliary input. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, volume 8349 of *Lecture Notes in Computer Science*, pages 566–590. Springer, 2014. 32

[Khu17] Dakshita Khurana. Round optimal concurrent non-malleability from polynomial hardness. In Kalai and Reyzin [KR17], pages 139–171. 1

[KR17] Yael Kalai and Leonid Reyzin, editors. *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, volume 10678 of *Lecture Notes in Computer Science*. Springer, 2017. 50

[KS17] Dakshita Khurana and Amit Sahai. Birthday simulation from exponential hardness: 2 round non-malleable commitments and 3 round gap zk. 2017. 1, 7, 11

[KY18] Ilan Komargodski and Eylon Yogev. Another step towards realizing random oracles: Non-malleable point obfuscation. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 259–279. Springer, 2018. 6

[Lev87] Leonid A. Levin. One-way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, 1987. 3, 52

[LP] Huijia Lin and Rafael Pass. Constant-round Non-malleable Commitments from Any One-way Function. In *STOC 2011*, pages 705–714. 1

[LP09] Huijia Lin and Rafael Pass. Non-malleability Amplification. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, STOC '09, pages 189–198, 2009. 1, 6

[LP12] Huijia Lin and Rafael Pass. Black-box constructions of composable protocols without set-up. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 461–478. Springer, 2012. 3

[LPS17] Huijia Lin, Rafael Pass, and Pratik Soni. Two-round and non-interactive concurrent non-malleable commitments from time-lock puzzles. Cryptology ePrint Archive, Report 2017/273, 2017. http://eprint.iacr.org/2017/273. 1, 4, 5, 6, 11

[LPV] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. Concurrent Non-malleable Commitments from Any One-Way Function. In *TCC 2008*, pages 571–588. 1, 17, 20

[PPV08] Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan. Adaptive One-Way Functions and Applications. In *Advances in Cryptology — CRYPTO '08*, pages 57–74, 2008. 1, 3, 6, 24

[PR05a] Rafael Pass and Alon Rosen. Concurrent Non-Malleable Commitments. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of ComputerScience*, FOCS '05, pages 563–572, 2005. 1

[PR05b] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In *STOC 2005*, pages 533–542, 2005. 16

[PR08] Rafael Pass and Alon Rosen. New and Improved Constructions of Nonmalleable Cryptographic Protocols. *SIAM J. Comput.*, 38(2):702–752, 2008. 1

[PW10] Rafael Pass and Hoeteck Wee. Constant-round non-malleable commitments from sub-exponential one-way functions. In *EUROCRYPT 2010*, pages 638–655, 2010. 1, 3, 12, 18, 19

[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. In *FOCS 2010*, pages 531–540, 2010. 1, 6

# A Two Message Arguments from Quantum Polynonial Hardness

In this section, we construct a two-message argument system assuming quantum (polynomial) hardness of LWE and polynomial hardness of factoring or discrete log. Recall that an argument system is a proof system where soundness holds only against computationally bounded (polynomial-size) provers.

The argument system we construct satisfies zero-knowledge with super-polynomial simulation and witness indistinguishability, as well as weak zero-knowledge, strong witness indistinguishability and witness hiding against delayed-input verifiers.

This argument system is the same as the one in [JKKR17], except that while the [JKKR17] protocol relies on any commitment and any two-message OT with security against unbounded receivers and *super-polynomial senders*, we rely on commitments based on factoring or discrete log [Lev87] and OT based on LWE [BD18] with security against unbounded receivers and quantum polynomial senders. This allows us to use quantum supremacy instead of complexity leveraging to argue soundness of the protocol.

## A.1 Modified Blum Protocol

We use a specific instantiation of the Blum $\Sigma$-protocol for Graph Hamiltonicity. Recall that in the Blum protocol, the prover commits to a random permutation and the permuted graph. If the verifier's challenge bit is $0$, the prover decommits to the permutation, and if the bit is $1$, decommits to a Hamiltonian cycle in this permuted graph. In our setting, instead of using *any* commitment, we will use a statistically binding, quantum-breakable non-interactive commitment[31]. Quantum breakable commitments are statistically binding (string) commitments that are computationally hiding against polynomial-size receivers, but where the value committed to by any malicious PPT committer can be extracted in quantum polynomial time. As described in Section 4.2, such a scheme exists based on any one-way function that is invertible in $\mathsf{BQP}$, such as one based on factoring or discrete log.

This protocol has soundness at least $\frac{1}{2} - \mathsf{negl}(n)$ against quantum polynomial-size provers, and satisfies honest-verifier zero-knowledge against PPT verifiers.

## A.2 Construction of Two-message Arguments

Our two-message argument is essentially identical to the one in [JKKR17, BGI+17][32]. Recall that these protocols use two-message oblivious transfer (OT) with super-polynomial security to convert the Blum $\Sigma$-protocol into a two-message argument system. We will use the modified Blum protocol above together with polynomially secure OT which is based on LWE.

Let $\mathsf{OT}_Q = (\mathsf{OT}_{Q,1}, \mathsf{OT}_{Q,2})$ denote a two-message bit oblivious transfer protocol. Let $\mathsf{OT}_{Q,1}(b)$ denote the first (receiver) message of this $\mathsf{OT}$ protocol with receiver input $b$, and let $\mathsf{OT}_{Q,2}(m_0, m_1)$ denote the second (sender) message of the OT protocol with sender input bits $m_0, m_1$[33]. We require this protocol to satisfy the following properties:

- The distributions $\mathsf{OT}_{Q,1}(0)$ and $\mathsf{OT}_{Q,1}(1)$ are computationally indistinguishable.

[31] These can be non-interactive or 2-message commitment; we rely on non-interactive commitments for simplicity.

[32] The only difference is that we use specific LWE-based OT and specific commitments, whereas they rely on super-polynomially secure OT and any commitment.

[33] We note that the second (sender) message also depends on the first (receiver) message; we omit this dependence here for succinctness.

- For every unbounded malicious receiver that outputs first message $o_1$, there exists a bit $b$ such that for every pair of messages $(m_0, m_1)$, the distributions $\mathsf{OT}_{Q,2}(m_0, m_1)$ and $\mathsf{OT}_{Q,2}(m_b, m_b)$ are statistically indistinguishable.

This can be instantiated assuming quantum polynomial hardness of LWE [BD18].

Let $\Sigma = (a, e, z)$ denote the three messages of the modified Blum protocol, where $a$ denotes the message of our underlying (quantum-breakable) commitment. We will perform a parallel repetition of this protocol, thus for each $i \in [n]$, $(a_i, e_i, z_i)$ are messages corresponding to an underlying modified Blum protocol with a single-bit challenge (i.e., where $e_i \in \{0, 1\}$).

**Two-Message Argument**

- **Verifier Message:**
  - For every $i \in [n]$ do the following:
    - Sample challenge $e_i$ uniformly at random.
    - Compute $o_{1,i} = \mathsf{OT}_{Q,1,i}(e_i)$.
  - Send $\{o_{1,i}\}_{i\in[n]}$ in parallel.
- **Prover Message:**
  - Obtain input $x \in L$, witness $w$ such that $R_L(x, w) = 1$.
  - For every $i \in [n]$, do:
    - Emulate the honest prover of the Blum Protocol by sampling commitment $a_i$ and compute answers $z_i^0, z_i^1$ corresponding to verifier challenges $0$ and $1$ respectively.
    - Compute $o_{2,i} = \mathsf{OT}_{Q,2,i}(z_i^0, z_i^1)$.
  - Send $\{a_i, o_{2,i}\}_{i\in[n]}$.
- **Verifier Output:** For every $i \in [n]$ verifier $V$ recovers $z_i$ as the output of $(\mathsf{OT}_{Q,1,i}, \mathsf{OT}_{Q,2,i})$ for $i \in [n]$, and outputs accept if for all $i \in [n]$, $(a_i, e_i, z_i)_{i\in[n]}$ is an accepting transcript of the underlying modified Blum protocol.

Figure 4: Two Message Argument System for NP

**Theorem 4.** *Assuming quantum polynomial hardness of LWE, and polynomial hardness of factoring or discrete log, there exist two-message arguments with adaptive soundness against polynomial-sized quantum provers, and satisfying:*

- *Witness Indistinguishability and ZK with superpolynomial simulation against all malicious verifiers*
- *Distributional weak zero-knowledge, strong WI and witness hiding against delayed-input verifiers.*

*Proof. (Sketch)* In this proof sketch, we focus on proving soundness.

We note that the proof of secrecy follows directly from previous work [BGI+17, JKKR17]. This is because the protocol in [BGI+17, JKKR17] is proven secure assuming *any* two-round malicious OT with security against unbounded receivers, and *any* commitment; and we only change it to rely on a *specific* instantiation of two-round malicious OT and commitments.

To prove soundness, [BGI+17, JKKR17] relied on the fact that OT hides the receiver choice bit from *super-polynomial senders*. We show that super-polynomial assumptions are not required if we assume that the receiver's choice bit is hidden from quantum polynomial-sized machines.

We show that if the underlying commitment is quantum-breakable and if $\mathsf{OT}_Q$ hides the receiver choice bit from polynomial-sized quantum malicious senders, the protocol in Figure 4 satisfies adaptive soundness against polynomial-sized quantum provers.

We will prove this by contradiction. Fix any cheating quantum prover $P^*$ and any $p(n) = \frac{1}{\mathsf{poly}(n)}$, such that that with probability at least $p(n)$ over the randomness of sampling verifier message, for infinitely many $n \in \mathbb{N}$, $P^*$ outputs $x \notin L$ together with an accepting transcript for $x$ according to the protocol in Figure 4. We will construct a quantum polynomial-size reduction $R^{P^*}$ that on input $\{o_{1,i} \xleftarrow{\$} \mathsf{OT}_{1,i}(e_i)\}_{i\in[n]}$ for $e = e_1 e_2 \dots e_n \xleftarrow{\$} \{0,1\}^n$, with oracle access to $P^*$, outputs $\widetilde{e}$ such that with probability at least $\frac{1}{p(n)}$, $\widetilde{e} = e$ (contradicting the receiver security of the OT).

The reduction $R$ on input $\{o_{1,i}\}_{i\in[n]}$ does the following:

- Send $\{o_{1,i}\}_{i\in[n]}$ to $P^*$ and obtain $\{a_i\}_{i\in[n]}$.
- Break the quantum breakable commitments $\{a_i\}_{i\in[n]}$ to obtain $\{v_i\}_{i\in[n]}$.
- Compute the string $\widetilde{e}$ as follows:
  1. For all $i \in [n]$, if $v_i$ consists of $(\pi, G')$ such that $G' = \pi(G)$, set $\widetilde{e}_i = 0$.
  2. Else set $\widetilde{e}_i = 1$.
- Output $\widetilde{e} = \widetilde{e}_1, \dots \widetilde{e}_n$.

Recall that $P^*$ breaks soundness with probability $p = \frac{1}{\mathsf{poly}(n)}$ for infinitely many $n \in \mathbb{N}$. This means that over the randomness of sampling $e$, $P^*$ outputs $x \notin L$ and $a_i^*, \mathsf{OT}_2(z_i^0, z_i^1)$ for $i \in [n]$ that cause the verifier to accept with probability $p$.

Moreover, whenever $x \notin L$ (that is, the corresponding Graph $G$ does not contain any Hamiltonian Cycle) and the transcript is accepting, then for every $i \in [n]$, either

- The committed graph is a correctly permuted variant of $G$. Since the transcript is accepting, this implies that $e_i = 0$, and note that in this case we set $\widetilde{e}_i = 0$, or
- The committed graph consists of a Hamiltonian cycle. Since the transcript is accepting, this implies that $e_i = 1$, and note that in this case we set $\widetilde{e}_i = 1$.

Therefore, in any accepting transcript where $x \notin L$, it must hold that $\widetilde{e} = e$.

Since $P^*$ outputs $x \notin L$ and an accepting proof for $x$ with probability at least $p(n)$ (for infinitely many $n \in \mathbb{N}$), it follows that $\widetilde{e} = e$ with probability at least $p(n)$ for infinitely many $n \in \mathbb{N}$, which contradicts receiver input-hiding security of the OT against polynomial-sized quantum machines. This completes the proof of soundness. □