Non-Malleable Codes Against Bounded Polynomial Time Tampering

Marshall Ball[1], Dana Dachman-Soled[2], Mukul Kulkarni[2], Huijia Lin[3], and Tal Malkin[1]

[1] Columbia University
{marshall,tal}@cs.columbia.edu
[2] University of Maryland
danadach@ece.umd.edu, mukul@umd.edu
[3] University of Santa Barbra
rachel.lin@cs.ucsb.edu

Abstract. We construct efficient non-malleable codes (NMC) that are (computationally) secure against tampering by functions computable in any *fixed* polynomial time. Our construction is in the plain (no-CRS) model and requires the assumptions that (1) **E** is hard for **NP** circuits of some exponential $2^{\beta n}$ $(\beta > 0)$ size (widely used in the derandomization literature), (2) sub-exponential trapdoor permutations exist, and (3) **P**-certificates with sub-exponential soundness exist.

While it is impossible to construct NMC secure against *arbitrary* polynomial-time tampering (Dziembowski, Pietrzak, Wichs, ICS '10), the existence of NMC secure against $O(n^c)$-time tampering functions (for any *fixed* c), was shown (Cheraghchi and Guruswami, ITCS '14) via a probabilistic construction. An explicit construction was given (Faust, Mukherjee, Venturi, Wichs, Eurocrypt '14) assuming an *untamperable* CRS with length longer than the runtime of the tampering function. In this work, we show that under computational assumptions, we can bypass these limitations. Specifically, under the assumptions listed above, we obtain non-malleable codes in the plain model against $O(n^c)$-time tampering functions (for any fixed c), with codeword length independent of the tampering time bound.

Our new construction of NMC draws a connection with non-interactive non-malleable commitments. In fact, we show that in the NMC setting, it suffices to have a much weaker notion called *quasi non-malleable commitments* — these are non-interactive, non-malleable commitments in the plain model, in which the adversary runs in $O(n^c)$-time, whereas the honest parties may run in longer (polynomial) time. We then construct a 4-tag quasi non-malleable commitment from any sub-exponential OWF and the assumption that **E** is hard for some exponential size **NP**-circuits, and use tag amplification techniques to support an exponential number of tags.

1 Introduction

Non-Malleable Codes (NMC) were introduced by Dziembowski, Pietrzak, and Wichs [DPW10] as a modification of error correcting codes, with the goal of achieving security against adversarial tampering functions, that may change every part of a codeword. Informally, a NMC against a class $\mathcal{F}$ guarantees that if a codeword is tampered via the application of a function $f \in \mathcal{F}$, then the decoding of the tampered codeword will either be exactly the original message, or completely unrelated to the original message. As noted in [DPW10], it is impossible to construct NMC against arbitrary tampering functions, since non-malleability can always be broken by a tampering function which first decodes the codeword to learn the underlying message, then re-encodes a related message. In particular, there can be no efficient NMC against arbitrary polynomial time tampering. Thus, to achieve feasibility, we must restrict the class of tampering functions.

A natural way to restrict tampering adversaries is via well-studied computational complexity measures. Several recent works have followed this approach and have developed strong connections between NMC and techniques from computational complexity. For example, Ball et al. [BDKM16] constructed NMC against bounded depth circuits with constant fan-in (which includes NC^0), several works [CL17, BDKM18,

BDSG⁺18] constructed NMC against AC^0 relying on different complexity theoretic techniques, and some works considered (restricted variants of) NMC against space-bounded tampering [FHMV17, BDKM18]. Specifically, the work of Faust et al. [FHMV17] considers space-bounded tampering adversaries in the random oracle model and achieves the security notion of *leaky* continuous non-malleability. The work of Ball et al. [BDKM18] is information-theoretic, considers streaming, space-bounded tampering adversaries and achieves standard non-malleability. The current work continues this line of research.

In this paper, we focus on the task of constructing NMC against *bounded* polynomial time tampering, namely tampering functions that are computable in an arbitrary *fixed* polynomial time. This is a very natural class to consider given the impossibility result for (unbounded) polynomial time, and indeed, some of the first works in this line of research have already considered this class. We discuss these next, along with the motivation and goals for our current work.

Cheraghchi and Guruswami [CG14] gave probabilistic constructions of efficient codes for circuits of size $O(n^c)$ (where an efficient randomized procedure outputs a "good" code with high probability). Faust et.al [FMVW14] gave an improved (in terms of the dependence on the error bound) construction against the same class, which is explicit, but relies on a model including an untamparable CRS (common reference string). The presence of CRS is undesirable, as not only must the CRS be generated by a trusted party, the CRS is also a non-tamperable component of the scheme. Moreover, both of these works can be viewed as using limited (t-wise) independence to partially derandomize probabilistic constructions. This approach inherently leads to a CRS whose length is at least as long as the bound on the size of the tampering circuits — meaning the tampering circuits cannot even read the entire CRS. We additionally note that if we allowed other size parameters, in particular the codeword size, to be as large as the runtime of the tampering function, then achieving non-malleability would become trivial. This motivates the following questions:

> *Can we construct efficient NMC against bounded polynomial time adversaries, in the* plain *model (i.e.* without *CRS)? Ideally, with codeword length that is independent of the runtime of the adversarial tampering function?*

As we elaborate next, we achieve this by moving to computational security and restricting our attention to uniform adversaries (while [CG14, FMVW14] gave statistical guarantees against non-uniform adversaries). In addition, as explained shortly below, we allow uniform bounded polynomial time tampering adversaries to have an inverse polynomial *advantage* (as in [CG14]) as opposed to having only negligible *advantage* (as in [FMVW14]). We emphasize that to the best of our knowledge, there is no transformation that either (a) eliminates the CRS in the NMC of [FMVW14] to achieve security against uniform (or non-uniform) adversaries or (b) fully derandomizes the monte carlo construction of [CG14], *even* under derandomization assumptions. Our techniques highlight interesting new connections to complexity theory.

1.1 Our Results

Our construction requires a complexity theoretic assumption that some language in the complexity class **E** (the class of languages that can be decided by Turing machines running in time $2^{O(n)}$) is hard for **NP** circuits of some exponential $2^{\beta n}$ (for $\beta > 0$) size. As surveyed later, such assumptions are widely used in the derandomization literature, often referred to as *derandomization assumptions*, and have connection with cryptography. Our construction also relies on the following cryptographic assumptions: the existence of subexponential trapdoor permutations and **P**-certificates (**P**-cert) with sub-exponential soundness. **P**-certs (introduced by [CLP13]) are "succinct" non-interactive arguments for languages $\mathcal{L} \in \mathsf{P}$, with proof length which is a fixed polynomial, independent of the time it takes to decide $\mathcal{L}$ (see Section 2.4 for a formal definition). We provide more background on these assumptions in Section 1.2 below.

Theorem 1 (Informal). *Assuming*

- **E** *is hard for* **NP** *circuits with some exponential size (namely $2^{\beta n}$ for some constant $\beta > 0$)*
- *Existence of sub-exponential trapdoor permutation*

2

– *Existence of $\mathbf{P}$-cert with sub-exponential soundness*

for every constant c_A, there is an efficient construction of NMC in the plain (no-CRS) model against uniform, bounded polynomial n^{c_A}-time tampering adversaries, with inverse polynomial indistinguishability (for any polynomial time non-uniform distinguisher). Furthermore, the codeword size is a fixed polynomial independent of n^{c_A}.

A few remarks are in order. First, to formalize that a tampered codeword, if not copied from the orginal codeword, must decode to an independent value, the definition of non-malleability requires that the decoded values, u_1 and u_2, obtained from tampering codewords of different values, v_1 and v_2 respectively, must be indistinguishable (u_b is replaced by same in the case of copying). Our NMC achieves inverse polynomial distinguishing advantage against polynomial-time non-uniform distinguishers .

Second, as mentioned before, it is important that the length of the codeword is smaller than the time-bound n^{c_A} of the tampering functions; otherwise, achieving non-malleability becomes trivial. Here, we achieve the ideal case, where the *length* of the codeword is bounded by a fixed polynomial, independent of n^{c_A}. As the adversarial time bound grows, the only parameter that grows is the *run time* of encode/decode. Moreover, this dependence is *necessary* as discussed earlier, since non-malleability is trivially impossible when the class of tampering functions includes the encode/decode functions.

Finally, we note that the assumption of the existence of sub-exponential trapdoor permutation in Theorem 1, can be replaced with the assumption of the existence of ZAPs (public coin, two message witness indistinguishable protocols) [DN00] with witness indistinguishability against sub-exponential adversaries and the existence of sub-exponential one-way functions (OWF). Note that ZAPs can be constructed from bilinear maps [GOS06], which are not known to imply trapdoor permutations.

Connection between NMC and Non-Malleable Commitments. Our construction of NMC draws a connection with another important notion of non-malleability – non-malleable commitments [DDN03, LPV08]. The only difference between NMC and non-interactive non-malleable commitments is that the former can be decoded efficiently, whereas decommitment of the latter cannot be done efficiently. A few prior works leverage this connection, showing that NMC can be used to obtain improved non-malleable commitments [GPR16, CGM$^+$16], and using techniques from the non-malleable commitment literature to obtain NMC [CGL16, OPVV18]. However, the latter direction—tapping into the wealth of techniques from the non-malleable commitment literature to construct NMC—has been largely unexplored, perhaps due to the fact that NMCs are typically unconditionally secure.

In our NMC construction, we begin with the framework of Ball et al. [BDKM18], which provides a generic way to construct NMC against tampering classes $\mathcal{F}$ for which sufficiently strong average-case hardness results are known, but requires a CRS. We show how to remove the CRS for particular tampering classes, including the class of bounded, poly-time adversaries. One modification is replacing the public key encryption scheme in the framework of [BDKM18] (whose pubic keys are contained in the CRS) with a non-interactive, non-malleable commitment scheme NMCom in the plain model.

At a very high (and overly simplified) level, our NMC, like [BDKM18], follows the Naor-Yung [NY90] paradigm that achieves CCA security of encryption, by composing two instances $\mathsf{Encrypt}(\mathrm{PK}, v), \mathsf{Encrypt}(\mathrm{PK}', v)$ of a public key encryption scheme, followed by a NIZK proof of the equality of encrypted values. In the context of NMC, we replace one instance of encryption with an encoding $\mathsf{E}(v)$ that is decodable in some polynomial t time, but has certain complexity theoretic hardness (specified shortly) against the class of circuits of smaller $t' < t$ size. We further replace the other instance of encryption with a non-malleable commitment c to v. Following [NY90, BDKM18], we provide a reduction that can turn any successful tampering adversary A against NMC, into an adversary B able to "maul" an encoding $\mathsf{E}(v)$ of v into a non-malleable commitment $\tilde{c}$ to a related value $\tilde{v}$. The challenge lies in ensuring that the reduction is "simple", namely, can be implemented by a circuit of size t'. Then the complexity theoretic hardness that we rely on is that it is impossible for such a circuit to compress an encoding $\mathsf{E}(v)$ into a much *shorter* string $\tilde{c}$ correlated to v (despite that the correlation may take exponential time to verify). Such an encoding, E, can be based on the incompressible functions of Applebaum et al. [AASY16], which can be constructed based on assumptions that are widely used in

the derandomization literature. (For more details on the NMC construction see the technical overview in Section 1.3).

Connection between Complexity Theory and Non-Malleable Commitments. Another contribution of this work, is to develop new connections between complexity theory and non-malleable cryptography. Specifically, we show that derandomization assumptions can be employed to build a new primitive we call Quasi Non-Malleable Commitments, which is weaker than standard non-malleable commitments, but nevertheless suffices for constructing NMC. This allows us to avoid adding the assumptions needed for standard non-interactive NMCom such as time-lock puzzles or hardness amplifiable injective one-way functions [LPS17, BL18].

Recall that in the setting of non-malleable codes, encode/decode can be in a larger complexity class than the adversary, and so standard non-interactive NMCom is an overkill. This motivates our definition of *Quasi Non-Malleable Commitmnes* in which the adversary runs in $O(n^{c_{com}})$-time, whereas the honest parties may run in longer (polynomial) time. To construct Quasi-NMCom from assumptions that are widely used in the derandomization literature, observe that these assumptions allow us to construct polynomial-time computable functions ψ for which non-deterministic advice does not help speed up the computation. This stands in stark contrast to the case of inversion of a one-way function ρ, which becomes easy with non-deterministic advice (as the advice can contain a pre-image). Following the framework of [LPS17], we construct two types of commitments that are *harder* than each other in different hardness "axes" — namely "BP-time" (corresponding to probabilistic Turing machines) and "non-deterministic (ND)-size" (corresponding to **NP**-circuits–see Sections 1.2 and 2.5). More specifically, one type of commitment com_1 are the standard schemes based on one-way functions ρ, and the other com_2 is based on the function ψ given by derandomization assumptions. The com_1 is much harder to break than com_2 in the axis of "BP-time", as inverting one-way function ρ is much harder than computing ψ using probabilistic Turing machines. On other hand, com_2 is much harder to break than com_1 in the axis of "ND-size", where both inverting ρ and computing ψ can be done in poly-size, but computing ψ is significantly harder.

From such mutually harder commitment schemes, we obtain a 4-tag Quasi-NMCom. Then, based on tag-amplification techniques in the literature [KS17b, BL18], we increase the number of tags supported to an exponential. It turns out that the *quasi*-setting makes amplification hard, which requires us to introduce a notion of "Double-Agent" adversaries. Informally, double-agent adversaries are probabilistic uniform Turing machines with "large" time complexity, that can also be represented as a distribution over circuits with "small" size complexity (see Section 2.1 for additional details). Post-amplification, our final Quasi-NMCom construction employs the same assumptions as Theorem 1. We believe these techniques may be useful for other applications in similar quasi-settings.

1.2 Background on Assumptions

In this section we provide some background on the assumptions that we use.

*On **P**-certificates.* **P**-certificates were introduced by [CLP13] in pursuit of constant-round concurrent zero-knowledge. Loosely, a **P**-certificate is a non-interactive proof system that allows a prover to convince an efficient verifier of the validity of any statement in **P** via a short proof. In particular, both the proof length and the run-time of the verifier are bounded by some fixed polynomial, but the system should work any language in **P** (the prover's efficiency should be comparable to the statement). CS-proofs [Mic00] imply **P**-certificates, but unlike the former, the latter assumption is falsifiable.

*On "**E** requires circuits of exponential size."* A fundamental family of questions in theoretical computer science is when and where randomness helps (vs strictly deterministic procedures). While it is widely believed that $\textbf{BPP} = \textbf{P}$ (i.e., any efficient, randomized decision procedure can be efficiently simulated by a deterministic procedure), whether the equality indeed holds is still an open problem. This particular question ($\textbf{BPP} = \textbf{P}$?) and others in the domain of *derandomization* have deep connections to cryptography.

In the 1980s, Yao [Yao82] showed that one-way permutations suffice to create pseudorandom generators (PRG) for poly-time computation. PRGs expand a small sequence of uniform random bits to a long sequence of pseudorandom bits that "fool" classes of procedures in the sense their behavior is essentially the same as if they were given truly random bits. In this sense, PRGs give a canonical technique for derandomizing decision procedures: running the procedure on multiple outputs of the PRG in parallel and taking majority of the obtained result. Later, it was shown that essentially minimal cryptographic assumptions (one-way functions) suffice for constructing PRGs [HILL99].

However, while most cryptography implies non-trivial derandomization, there seem to be inherent barriers to statements of the converse form. In fact, the so-called "cryptographic" PRG's yield, in two aspects, much more than what is required for derandomization since (a) the output of such PRGs fool *any* polynomial time procedure (including procedures that run in much more time than the PRG itself) and (b) such PRGs guarantee that the behavior of poly-time procedures is only negligibly different from their behavior on true randomness. On the other hand, one-way functions are not known to imply **P = BPP** because known constructions only "stretch" random bits into polynomially many random bits (whereas exponential stretch is required for canonical simulation).

Capitalizing on these observations, Nisan and Wigderson [NW94] gave a generic means of constructing PRGs which "fool" a certain class of circuits $\mathcal{C}$, from any function that is hard-on-average for a slightly enlarged class of circuits. In particular, this in some sense reduces the problem of explicit derandomization to proving strong circuit lower bounds on explicit functions. To this end, later work showed that, in fact, simply assuming there is a language in **E** that does not have have circuits size $2^{\beta n}$ for some $\beta > 0$ (for almost all n), is sufficient to derandomize BPP [IW97, STV01]. Moreover, because **E** has complete problems, this yields explicit pseudorandom generators. However, for reasons alluded to above, this assumption is, to best of our knowledge, incomparable to standard cryptographic assumptions.

This latter (worst-case) conjecture and its generalization has appeared in a variety of contexts pertaining to derandomization and other questions in computational complexity [Lip89, NW94, BFNW93, IW97, STV01, HN10, KVM02, SU06, SU09, FL97, MV05, TV00, SU05, GW02, GSTS03, Dru13].

The conjectures we are concerned with in this work take the following form (following [AASY16]):

Assumption 1 (E is hard for exponential size X-circuit) *There exists a problem* **L** *in* **E = DTIME**$(2^{O(n)})$ *and a constant $\beta > 0$, such that for every sufficiently large n, X-circuits of size $2^{\beta n}$ fail to compute the characteristic of* **L** *on inputs of length n.*

where X-circuits in Assumption 1 can be the circuits of type, {*non-deterministic, co-non-deterministic,* **NP**, Σ_i}. See section 2.5, for definitions of these types of circuits.

While these types of assumptions are independently interesting, in this work we will utilize some surprising implications outside of derandomization.

Recently, Applebaum et al. [AASY16] presented (explicit) constructions of poly-time computable incompressible functions based on the assumption that **E** is hard for exponential size non-deterministic circuits (based on the extractors for samplable distributions of Trevisan and Vadhan [TV00]). Loosely, a function, ψ is incompressible for a class if no procedure in that class can "shrink" an input to the function, x, such that $\psi(x)$ can later be recovered. Note that, to our knowledge, it is not known how to construct incompressible functions from standard cryptographic assumptions (unlike the case of derandomization).

Barak et al. [BOV07] observed that similar assumptions can be used to construct cryptographic primitives. In particular, they showed that if **E = DTIME**$(2^{O(n)})$ contains a function with *co-non-deterministic* circuit complexity $2^{\Omega(n)}$, then there exists (explicit) non-interactive witness indistinguishable proof systems for **L** $\in$ **NP** (additionally assuming the existence of trapdoor permutations). They also showed that the same assumption can be used to construct a non-interactive bit commitment scheme from a one-way function.

In this work, we use the above results and demonstrate new connections between these assumptions and non-malleable cryptography. In particular we show that if Assumption 1 holds for **NP**-circuits and (sub-exponential) one-way functions exist, then we can construct quasi-non-malleable commitment schemes. We combine our construction of such commitment schemes along with NIZK proofs based on the NIWI

of [BOV07], as well as the incompressible functions of [AASY16], to obtain our main result: a family of efficient non-malleable codes secure against tampering by uniform algorithms running in time $O(n^c)$.

1.3 Technical Overview

We begin by recalling (a simplified version of) the template for constructing non-malleable codes against complexity class $\mathcal{F}$ (based on the Naor-Yung double encryption paradigm [NY90]) introduced in the work of Ball et al. [BDKM18]:

The CRS contains a public key PK for an encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Encrypt}, \mathsf{Decrypt})$, and a CRS crs for a simulation-sound, non-interactive zero knowledge proof (NIZK). For $b \in \{0,1\}$, let $\mathcal{D}_b$ denote disjoint distributions over $x_1 \ldots x_n \in \{0,1\}^n$ such that $\psi(x_1 \ldots x_n) = b$, where ψ is poly-time computable, yet every $f \in \mathcal{F}$ has low correlation with ψ.

To encode a bit b:

1. Randomly choose string $x_1 \ldots x_n$ from $\mathcal{D}_b$
2. Compute $c \leftarrow \mathsf{Encrypt}_{\mathrm{PK}}(b)$.
3. Compute a NIZK proof T of "consistency": $\exists b' \in \{0,1\}$ s.t. $x_1 \ldots x_n$ is in the support of $\mathcal{D}_{b'}$ and b' is the plaintext underlying c.
4. Output $(x_1 \ldots x_n, c, T)$.

To decode $(x_1 \ldots x_n, c, T)$:

1. Verify the NIZK proof T.
2. If it accepts, output $\psi(x_1 \ldots x_n)$.

The proof of [BDKM18] proceeds (loosely) as follows: In the first hybrid they switch to simulated proof T'. Then they switch c, in the "challenge" encoding to an encryption of garbage c', and next switch to an alternative decoding algorithm *in $\mathcal{F}$*, which requires the trapdoor SK (corresponding to the public key PK which is contained in the CRS). If, in the final hybrid, decodings of tampered encodings depend on b, a circuit in $\mathcal{F}$ can be constructed, whose output is correlated with the hard function ψ, reaching a contradiction. While [BDKM18] do in fact show that the CRS can be removed for constructions against certain classes $\mathcal{F}$ of tampering, naively, their approach requires a CRS in two seemingly inherent ways: First, the CRS allows the use of the secret key trapdoor SK in the alternate decoding algorithm and second, it allows the use of a simulation-sound NIZK, which requires CRS.

In this work, we make two crucial observations that allow us to eliminate the CRS from the above construction. First, we consider a stronger notion of hardness for ψ, known as *incompressibility* (in fact, this hardness notion was already implicitly used in [BDKM18] for their multi-bit construction). Briefly, if a function ψ is incompressible by circuit class $\mathcal{C}$, it means that for $t \ll n$, for any (computationally unbounded) Boolean function $F : \{0,1\}^t \to \{0,1\}$ and any $C : \{0,1\}^n \to \{0,1\}^t \in \mathcal{C}$, the output of $F \circ C(x_1, \ldots, x_n)$ is uncorrelated with $\psi(x_1, \ldots, x_n)$ (over uniform choice of $x_1, \ldots, x_n$). Now, since F is allowed to be computationally unbounded, we may consider an F that decrypts the ciphertext $c = \mathsf{Encrypt}_{\mathrm{PK}}(b)$ by brute force search. To elaborate, instead of using SK to efficiently decrypt c in complexity class $\mathcal{C}$, the alternate decoding algorithm D' is split into two parts $\mathsf{D}' = \mathsf{D}'_2 \circ \mathsf{D}'_1$, where D'_1 can be implemented in $\mathcal{F}$, but has short output length, whereas D'_2 is computationally unbounded. Specifically, D'_1 checks the proof T and then outputs the entire ciphertext c (which is fine so long as the length of c is sufficiently smaller than n), and, due to the incompressibility property of ψ, we must still have that the output of $\mathsf{D}' = \mathsf{D}'_2 \circ \mathsf{D}'_1$ is uncorrelated with $\psi(x_1, \ldots, x_n)$. This eliminates the need of providing a trapdoor to the alternate decoding algorithm and so instead of using a public key encryption scheme, we may use a non-interactive statistically binding commitment scheme, which can be constructed from injective one-way function or from derandomization assumptions and any one-way function [BOV07].[4]

---

[4] As we will see, in our setting of non-malleable codes against polynomially-bounded adversaries, our construction requires such derandomization assumptions in any case and so only standard one-way function is required in addition. However, for simplicity we will assume injective one-way function in the remainder of the exposition in this section.

Next, we note that it is possible to construct a NIZK proof system in the plain (no-CRS) model (i.e. "One-Message Zero Knowledge"), with soundness against uniform adversaries. To do so, one first constructs a non-interactive witness indistinguishable proof system (NIWI) in the plain model (based on standard cryptographic assumptions and derandomization assumptions [BOV07]) and then converts from witness indistinguishability to full zero knowledge using the well-known FLS paradigm [FLS99]. Specifically, the simulator will be given a trapdoor witness based on a problem that is computationally hard for *uniform* PPT adversaries such as finding a collision in a keyless collision resistant hash function. The problem with this approach is that in the proof sketch outlined above, we actually require *simulation-sound* NIZK, as opposed to regular NIZK. In simulation-sound NIZK, the soundness properties must hold, even after the adversary sees a simulated proof of a false statement. Whereas various constructions of (one-time) simulation-sound NIZK rely on embedding a trapdoor within the CRS (cf. [Sah99, Lin03]), our approach to achieve the simulation-soundness property without CRS is to replace the commitment c (which replaced the encryption $\mathsf{Encrypt}_{\mathrm{PK}}(b)$ as described above) with a *non-interactive, non-malleable* commitment scheme. Unfortunately, currently known non-interactive, non-malleable commitment schemes require somewhat non-standard assumptions such as time-lock puzzles or hardness amplifiable injective one-way functions [LPS17, BL18], whereas our goal is to minimize assumptions. As we will see, the fact that our commitment scheme is only required to be non-malleable against adversaries in a restricted circuit class $\mathcal{F}$, allows us to obtain non-interactive, non-malleable commitments, while reducing assumptions.

Instantiating the Paradigm In this work we construct non-malleable codes against the class $\mathcal{F}$ of uniform, polynomial-bounded tampering functions. Crucially, we will do so (1) *without* relying on CRS (2) with codeword length that is independent of the polynomial time bound (note that if the codeword length is longer than the polynomial time bound then the adversary does not even get to read the entire input, also it's trivial to construct these) and (3) while reducing computational assumptions, to the extent possible.

Specifically, in addition to standard cryptographic assumptions, we will assume standard derandomization-type assumptions such as those discussed in the previous section. We also require the notion of **P**-certificates, which seem to be necessary to implement the above high-level paradigm, as we discuss next. To see why this is so, note that the statement proved in NIZK proof T, involves proving that $\psi(x_1, \ldots, x_n)$ is equal to some value. Note that ψ is a polynomial-time computable function, but that intrinsic in the approach is choosing ψ that is hard to compute in the specific polynomial time bound $T(n)$ corresponding to tampering class $\mathcal{F}$. Moreover, we require that the size of the proof T be independent of the polynomial time bound $T(n)$, and so in particular the size of the proof T must be independent of the time required to compute ψ. This is now exactly the notion of a **P**-certificate.

We also note that given the above paradigm for encoding of a single bit, it is straightforward to obtain a scheme for the encoding of multiple bits (by individually encoding each bit and then using a single proof T to "wrap" together the individual encodings). The only restriction will be that the number of bits, m, that are encoded, multiplied by the length of a bit commitment, λ, should be sufficiently smaller than n, the input length of the function ψ. See Section 3 for additional details.

Instantiation of ψ Recall that for the above approach to work, we must instantiate ψ with a function that is incompressible against polynomially-bounded adversaries. Fortunately, such a construction was given by [AASY16], based on a derandomization-type assumption. See Section 5 for additional details.

Instantiation of NMCom In fact, as discussed previously, we note that we do not need full-fledged NMCom, but only *Quasi* NMCom, i.e. NMCom with the following two relaxations: (1) The commitment scheme is only secure against bounded-poly (in fact "Double-Agent") adversary and distinguisher (2) The complexity of the honest sender/receiver may be greater than the complexity of the adversary. To construct Quasi-NMCom, we adopt the approach of [LPS17] to initially construct a commitment scheme with small number of tags, and use the fact that the derandomization assumptions that we employ in this work are believed to hold even against *non-deterministic* adversaries. In particular, we employ the well-studied assumption that **E** is

hard for adversaries represented as exponential size **NP**-circuits—or circuits with access to a SAT oracle (See Sections 1.2 and 2.5 for further discussions on these assumptions). To construct our NMCom scheme, we start off with two different types of commitments, Type 0 and Type 1 such that if we get a Type 0 on left, we can extract from Type 1 on the right without breaking the security of Type 0 and vice versa. Each commitment consists of an input x to a Boolean function ψ' (with logarithmic input length) that is hard for **NP**-circuits of size $2^{\epsilon_3 \cdot \text{input length}}$ to compute as well as the output y of an injective OWF ρ, which is hard for ppt adversaries running in time $2^{\text{input length}^{\epsilon'_3}}$.[5] Each of these can be considered as a commitment to a bit (given x, the output of $\psi'(x)$ is the committed value and given y, a hardcore bit of ρ) and the final committed value is the xor of the two bits committed.

Type 0: input length $c_1 \log(n)$ to ψ', input length $n^{\epsilon'_1}$ to ρ.
Type 1: input length $c_2 \log(n)$ to ψ', input length $n^{\epsilon'_2}$ to ρ.

Set $c_2 > c_1 > \epsilon'_1 > \epsilon'_2$ so that

1. $n^{c_1} < n^{\epsilon_3 \cdot c_2}$
2. $2^{n^{\epsilon'_2}} < 2^{n^{\epsilon'_3 \cdot \epsilon'_1}}$

We now consider the two possible cases:

Type 0 on left, Type 1 on right. Extract by inverting the injective OWF ρ in deterministic time $2^{n^{\epsilon'_2}}$ and computing ψ' in deterministic time n^{c_2}. Note that this does not allow breaking injective OWF ρ with input length $n^{\epsilon'_1}$, which is secure against time $2^{n^{\epsilon'_3 \cdot \epsilon'_1}} > 2^{n^{\epsilon'_2}}$.

Type 1 on left, Type 0 on right. Extract by computing ψ' in deterministic time n^{c_1} and inverting the injective OWF ρ with an **NP**-circuit of size $n^{\epsilon'_1}$. Note that this does not allow breaking hardness of ψ' with input length $c_2 \log(n)$, which is secure against **NP**-circuits of size $n^{\epsilon_3 \cdot c_2} > n^{c_1}$.

See Figure 1 for a summmary and Section 6 for additional details.

	Input length to ψ'	Hardness of ψ'		Input length to ρ	Hardness of ρ	
		D	ND		D	ND
Type 0	$c_1 \cdot \log(n)$	$n^{\epsilon_3 \cdot c_1}$	$n^{\epsilon_3 \cdot c_1}$	$n^{\epsilon'_1}$	$2^{n^{\epsilon'_3 \cdot \epsilon'_1}}$	$n^{\epsilon'_1}$
Type 1	$c_2 \cdot \log(n)$	$n^{\epsilon_3 \cdot c_2}$	$n^{\epsilon_3 \cdot c_2}$	$n^{\epsilon'_2}$	$2^{n^{\epsilon'_3 \cdot \epsilon'_2}}$	$n^{\epsilon'_2}$

Fig. 1. ψ' and ρ are the functions described in the paragraph above. D stands for deterministic and ND stands for "non-deterministic" hardness. We set parameters so that $c_2 > c_1 > \epsilon'_1 > \epsilon'_2$.

The above 2-tag commitment scheme can then be straightforwardly extended to work for 4 tags, at which point amplification techniques from [KS17b] can be applied to obtain NMCom with number of tags exponential in the security parameter. The analysis of the amplified scheme is somewhat different than in prior work, since our analysis must carefully take into account that some assumptions are inherently uniform (One-Message Zero Knowledge) and some assumptions (hardness of ψ') are inherently non-uniform (the adversary in the proof is so limited that it does not have time to *generate* new commitments on its own and therefore must receive them as non-uniform advice when reducing security to the hardness of computing ψ'). To solve this problem, we introduce the notion of "Double Agent" adversaries (as discussed in the introduction) and provide a proof of security of our amplified NMCom scheme against this class of adversaries. See Section 7 for additional details.

---

[5] For this exposition, we assume for simplicity that ψ' can be computed in deterministic time $2^{\text{input length}}$ and that the injective OWF has linear circuit size. Recall that we do not require injective OWF and that any statistically binding, non-interactive commitment scheme is sufficient, but that for simplicity we assuming injective OWF in this exposition.

1.4 Related Work

Non-Malleable Codes. Non-malleable codes (NMC) were introduced by Dziembowski, Pietrzak and Wichs in their seminal work [DPW10]. While there has been a long line of important results for various tampering classes, due to space limitations, we discuss here only the results most relevant to this work.

As discussed extensively in the introduction, Faust et.al [FMVW14] constructed efficient information-theoretically secure NMC in the CRS model, resilient against tampering function classes $\mathcal{F}$ which can be represented as circuits of size $\mathsf{poly}(n)$. Another important result by Cheraghchi and Guruswami [CG14] showed the existence of information theoretically secure NMC against tampering families $\mathcal{F}$ of size $|\mathcal{F}| \leq 2^{2^{\alpha n}}$ with optimal rate $1 - \alpha$. They achieve error $\varepsilon \in O(1/\mathsf{poly}(n))$ as the run-time of the encoding and decoding algorithms is proportional to $\mathsf{poly}(1/\varepsilon)$ where ε is the error probability.

Ball et.al [BDKM16] constructed efficient information theoretic secure NMC against n^δ-local tampering functions, for any constant $\delta > 0$. This class includes tampering functions, which can be represented as constant depth circuits with bounded fan-in i.e NC^0 circuits. Chattopadhyay and Li [CL17] constructed NMC against AC^0 tampering functions from seedless non-malleable extractors, although the codeword length of this construction is super-polynomial in the message length n. Faust et.al [FHMV17] considered non-malleable codes against space bounded tampering adversaries in the random oracle model. The construction achieves a new notion of *leaky* continuous non-malleable codes (with self-destruct property), where the adversary is allowed to learn some bounded $\log(|m|)$ bits of information about the underlying message m.

Recently, Ball et.al [BDKM18] presented a generic framework to construct NMC against tampering function classes for which average-case hardness bounds are known. They also instantiated their framework to construct the first efficient, computationally secure multi-bit NMC against tampering functions which can be represented as constant-depth circuits with unbounded fan-in (AC^0 tampering), as well as against tampering functions which can be represented as bounded depth decision tree. Additionally, they showed that the framework can be used to construct information-theoretic NMC against space-bounded streaming tampering. Information-theoretic secure, efficient NMC against AC^0 tampering were subsequently constructed by [BDSG$^+$18].

Derandomization and Cryptography The connection between derandomization techniques with cryptography was first explored by Barak et.al. [BOV07], who constructed one-message witness indistingushable proof systems (non-interactive commitment scheme) in the plain model based on trapdoor permutations (one-way functions) in addition to the derandomization assumptions. Recently, Applebaum et.al. [AASY16] constructed incompressible functions against the class of bounded polynomial time functions from similar assumptions.

Non-Malleable Commitments Non-malleable commitments have been studied extensively since their introduction by [DDN03] in their seminal paper. Great progress has been made in reducing the interaction between the sender and the receiver, while minimizing computational assumptions. We list just some of the results in this line of work [Bar02, PR05a, PR05b, LP09, PW10, Goy11, LP11, GRRV14, GPR16, COSV16, COSV17, Khu17]. Recently, Lin, Pass, and Soni [LPS17] gave a construction of a non-interactive, fully-concurrent, non-malleable commitment scheme secure against uniform adversaries based on sub-exponential non-interactive commitment schemes, non-interactive witness indistingushable proof systems (NIWI), uniform collision resistant hash functions, and time-lock puzzles [RSW96]. When replacing the uniform collision resistant hash functions with a family of collision resistant hash functions, their protocol becomes 2-round. Khurana and Sahai [KS17b] constructed 2-round non-malleable commitments with bounded concurrency from standard sub-exponential assumptions. Bitansky, and Lin [BL18] gave a construction of a non-interactive, fully-concurrent, non-malleable commitment scheme from multi-collision-resistant keyless hash functions, sub-exponentially-secure time-lock puzzles, and other standard assumptions.

2 Definitions

2.1 Notation

When comparing distribution ensembles $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}, \mathcal{D}' = \{\mathcal{D}'_n\}_{n \in \mathbb{N}}$, we use the notation $\mathcal{D} \overset{\mathcal{G},\mathcal{S}}{\approx} \mathcal{D}'$, where $\mathcal{G}, \mathcal{S}$ are sets, to indicate that for sufficiently large n, every distinguisher $D \in \mathcal{G}$ distinguishes $\mathcal{D}_n$ from $\mathcal{D}'_n$ with probability at most $p(n)$, for some $p(\cdot) \in \mathcal{S}$. When comparing functions p, p', we use the notation $p(n) \overset{\mathcal{S}}{\approx} p'(n)$, where $\mathcal{S}$ is a set, to indicate that $|p(n) - p'(n)| \in \mathcal{S}$.

We consider "Double-Agent" adversaries A in computational classes denoted by $\mathbf{BPtime}(T(n)) \bigcap \mathbf{SIZE}(t(n))$, for some functions $T(\cdot)$, $t(\cdot)$. Intuitively, this computational class contains probabilistic uniform Turing machines A with "large" time complexity $T(n)$, that can also be represented as a distribution over circuits with "small" size complexity $t(n)$. Informally, this is possible since A can be split into subroutines in such a way that subroutines that require "large" time complexity can all be replaced with non-uniform advice. Formally, $A \in \mathbf{BPtime}(T(n)) \bigcap \mathbf{SIZE}(t(n))$ if the following hold:

- $A = (A_1, A_2)$.
- $A_1 \in \mathbf{BPtime}(T(n))$, $A_2 \in \mathbf{BPtime}(t(n))$.
- A_1 receives only security parameter 1^n as input and produces output of length at most $t(n)$.
- A_2 receives the input of A as its input, along with the output of A_1.

Note that, since A_1 takes only security parameter as input, the output of A_1, can be viewed as non-uniform advice to A_2. Thus, we can convert such a uniform adversary $A = (A_1, A_2)$ into a distribution over non-uniform circuits of size $t(n)$ with identical behavior to A.

2.2 Non-Malleable Codes

Definition 1 (Coding Scheme). *Let* $\Sigma, \widehat{\Sigma}$ *be sets of strings, and* $\kappa, \widehat{\kappa} \in \mathbb{N}$ *be some parameters. A coding scheme consists of two algorithms* (E, D) *with the following syntax:*

- *The encoding algorithm* (perhaps randomized) *takes input a message in* Σ *and outputs a codeword in* $\widehat{\Sigma}$.
- *The decoding algorithm takes input a codeword in* $\widehat{\Sigma}$ *and outputs a message in* Σ.

We require that for any message $\mathsf{msg} \in \Sigma$, $\Pr[\mathsf{D}(\mathsf{E}(\mathsf{msg})) = \mathsf{msg}] = 1$.

Definition 2 ($O(1/p(n))$-Non-malleability [DPW10]). *Let* n *be the security parameter,* $\mathcal{F}$ *be some family of functions. For each function* $f \in \mathcal{F}$, *and* $\mathsf{msg} \in \Sigma$, *define the tampering experiment:*

$$\mathbf{Tamper}^f_{\mathsf{msg}} \overset{\mathrm{def}}{=} \left\{ \begin{matrix} c \leftarrow \mathsf{E}(\mathsf{msg}), \tilde{c} := f(c), \tilde{\mathsf{msg}} := \mathsf{D}(\tilde{c}). \\ Output: \ \tilde{\mathsf{msg}}. \end{matrix} \right\},$$

where the randomness of the experiment comes from the encoding algorithm. We say a coding scheme (E, D) *is* $O(1/p(n))$*-non-malleable with respect to* $\mathcal{F}$ *if for each* $f \in \mathcal{F}$, *there exists a PPT simulator* Sim *such that for any message* $\mathsf{msg} \in \Sigma$, *we have*

$$\mathbf{Tamper}^f_{\mathsf{msg}} \overset{PPT, O(1/p(n))}{\approx} \mathbf{Ideal}_{\mathsf{Sim},\mathsf{msg}} \overset{\mathrm{def}}{=} \left\{ \begin{matrix} \tilde{\mathsf{msg}} \cup \{\mathsf{same}^*\} \leftarrow \mathsf{Sim}^{f(\cdot)}. \\ Output: \mathsf{msg} \text{ if output of } \mathsf{Sim} \text{ is } \mathsf{same}^*; \\ \text{otherwise } \tilde{\mathsf{msg}}. \end{matrix} \right\}$$

Definition 3 ($O(1/p(n))$-Medium Non-malleability). *Let* n *be the security parameter,* $\mathcal{F}$ *be some family of functions. Fix* $\mathsf{msg} \in \Sigma$. *Let* $c \leftarrow \mathsf{E}(\mathsf{msg})$ *and let* $g(\cdot, \cdot)$ *be a predicate such that for every* $f \in \mathcal{F}$,

$$\Pr[g(c, f(c)) = 1] \wedge \mathsf{D}(f(c)) \neq \mathsf{msg}] \leq \mathsf{negl}(n).$$

For g as above, each function $f \in \mathcal{F}$, *and* $\mathsf{msg} \in \Sigma$, *define the tampering experiment*

$$\mathbf{MediumNM}^f_{\mathsf{msg},g} \;\overset{\mathrm{def}}{=}\; \left\{ \begin{array}{c} c \leftarrow \mathsf{E}(\mathsf{msg}), \tilde{c} := f(c), \tilde{\mathsf{msg}} := \mathsf{D}(\tilde{c}) \\ Output: \;\; \mathsf{same}^* \; if \; g(c,\tilde{c}) = 1, \;\; and \; \tilde{\mathsf{msg}} \; otherwise. \end{array} \right\}$$

The randomness of this experiment comes from the randomness of the encoding algorithm. We say that a coding scheme (E, D) is $O(1/p(n))$-medium non-malleable with respect to $\mathcal{F}$ if there exists a g as above and for any $\mathsf{msg}, \mathsf{msg}' \in \Sigma$ and for each $f \in \mathcal{F}$, we have:

$$\{\mathbf{MediumNM}^f_{\mathsf{msg},g}\}_{n\in\mathbb{N}} \;\overset{PPT, O(1/p(n))}{\approx}\; \{\mathbf{MediumNM}^f_{\mathsf{msg}',g}\}_{n\in\mathbb{N}}$$

It is straightforward to check that medium non-malleability implies standard non-malleability.

2.3 Non-Interactive Commitment Scheme

Definition 4 (Commitment Scheme). *A (non-interactive) commitment scheme for the message space* $\{0,1\}^m$, *is a pair* $(\mathsf{Com}, \mathsf{Open})$ *such that:*

- *For all* $\mathsf{msg} \in \{0,1\}^m$, $(c,d) \leftarrow \mathsf{Com}(m)$ *is the* commitment/opening *pair for the message* msg.
- $\mathsf{Open}(\mathsf{msg}, c, d) \to \{0,1\}$, *where 1 indicates that d is a valid opening of c to* msg *and 0 is returned otherwise.*

The commitment scheme must satisfy the standard correctness requirement,

$$\forall m \in \mathbb{N}, \forall \mathsf{msg} \in \{0,1\}^m, \; \Pr\left[\mathsf{Open}(\mathsf{msg}, \mathsf{Com}(\mathsf{msg})) = 1\right] = 1$$

where the probability is taken over the randomness of Com.

We will consider *statistically* binding commitment schemes. A non-interactive commitment scheme $\mathcal{C} := (\mathsf{Com}, \mathsf{Open})$ is statistically-binding if the following hold:

Hiding: It is computationally hard for any adversary $\mathcal{A}$ to generate two messages $\mathsf{msg}_0, \mathsf{msg}_1 \in \{0,1\}^m$ such that $\mathcal{A}$ can distinguish between their corresponding commitments. Formally, for any ppt adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ it should hold that:

$$\Pr\left[b = b' \;\middle|\; \begin{array}{c} (\mathsf{msg}_0, \mathsf{msg}_1, \alpha) \leftarrow \mathcal{A}_1(1^m), b \leftarrow_r \{0,1\}, \\ (c,d) \leftarrow \mathsf{Com}(\mathsf{msg}_b), b' \leftarrow \mathcal{A}_2(c, \alpha) \end{array}\right] \le \frac{1}{2} + \mathsf{negl}(m)$$

Statistical Binding: Formally, for any (unbounded) adversary $\mathcal{A}$ it should hold that:

$$\Pr\left[\mathsf{msg} \neq \mathsf{msg}' \;\middle|\; \begin{array}{c} (c, \mathsf{msg}, d, \mathsf{msg}', d') \leftarrow \mathcal{A}(1^m), \\ 1 \leftarrow \mathsf{Open}(\mathsf{msg}, c, d), 1 \leftarrow \mathsf{Open}(\mathsf{msg}', c, d') \end{array}\right] \le \mathsf{negl}(m)$$

Well-formed Commitments: Let $\mathsf{val}(\cdot)$ be a function which takes an arbitrary commitment c as an input. val outputs msg if $\exists$ unique msg such that $\mathsf{Open}(\mathsf{msg}, c, \cdot) = 1$, and outputs $\perp$ otherwise.

Definition 5 (Tag-based Commitment Scheme [LPS17]). *A commitment scheme* $(\mathsf{Com}, \mathsf{Open})$ *is a tag-based commitment scheme with $\tau(m)$ number of tags if, in addition to the the message msg, the sender (committer) and receiver also receive a "tag" of length* $\mathrm{poly}(\log(\tau(m)))$ *as common input.*

If $\tau(m)$ is exponential in security parameter m, we omit the prefix $\tau(m)$ and refer to the commitment scheme as simply a tag-based commitment scheme.

Man In The Middle Execution (MIM): Let $(\mathsf{Com}, \mathsf{Open})$ be a tag-based commitment scheme, and A an adversary. For security parameter m, consider the following interactions by $A(1^m)$:

- *Left interaction:* $A(1^m)$ interacts with the sender and receives commitment to a message msg of length m using identity tag as $c \leftarrow \mathsf{Com}(\mathsf{msg}, \mathsf{tag})$.
- *Right interaction:* $A(1^m)$ interacts with the receiver and tries to commit to related message $\tilde{\mathsf{msg}}$ using identity $\tilde{\mathsf{tag}}$ of its choice. Specifically, for the commitment $\tilde{c}$ sent to the receiver, let $\tilde{\mathsf{msg}} = \mathsf{val}(\tilde{c})$. Furthermore, if $\tilde{\mathsf{tag}} = \mathsf{tag}$, then we set $\tilde{\mathsf{msg}} = \bot$.

Let $\mathsf{mim}_{\mathcal{C}}^A(\mathsf{msg})$ denote the random variable that describes $\tilde{\mathsf{msg}}$ that A commits to in the right interaction along with its output in the MIM execution $\mathsf{MIM}_{\mathcal{C}}^A(\mathsf{msg})$ as described above.

Definition 6 ($O(1/p(m))$-Non-Malleability against $\mathcal{G}$ [LPS17]).

A tag-based commitment scheme $\mathcal{C} = (\mathsf{Com}, \mathsf{Open})$ is said to be $O(1/p(m))$-non-malleable against $\mathcal{G}$ if $\forall$ $A \in \mathcal{G}$, the following ensembles are indistinguishable,

$$\left\{\mathsf{mim}_{\mathcal{C}}^A(\mathsf{msg}_0)\right\}_{m \in \mathbb{N}, \mathsf{msg}_0 \in \{0,1\}^m} \overset{\mathcal{G}, O(1/p(m))}{\approx} \left\{\mathsf{mim}_{\mathcal{C}}^A(\mathsf{msg}_1)\right\}_{m \in \mathbb{N}, \mathsf{msg}_1 \in \{0,1\}^m}.$$

2.4 P-Certificates

We first define the notion of a **P**-certificate, introduced by [CLP13], and then discuss candidate instantiations of the assumption. The following exposition is based heavily on that of [CLP13].

Roughly speaking, we say that (P, V) is a **P**-certificate system if (P, V) is a non-interactive proof system (i.e., the prover sends a single message to the verifier, who either accepts or rejects) allowing an efficient prover to convince the verifier of the validity of any deterministic polynomial-time computation $M(x) = y$ using a "certificate" of some fixed polynomial length (independent of the size and the run-time of M) whose validity the verifier can check in some fixed polynomial time (independent of the run-time of M); that is, any deterministic polynomial-time computation can be certified using a "short" certificate that can be "quickly" verified.

Formally, we consider the following canonical languages for **P**: for every constant $c \in \mathbb{N}$, let $L_c = \{(M, x, y) : M(x) = y \text{ within } |x|^c \text{ steps }\}$. Let $T_M(x)$ denote the run-time of M on input x.

Definition 7 (P-certificate). *A pair of probabilistic interactive Turing machines, $(P_{\mathsf{cert}}, V_{\mathsf{cert}})$, is a **P**-certificate system if there exist polynomials g_P, g_V, ℓ such that the following holds:*

- Efficient Verification: *On input $c \geq 1$, 1^n and a statement $q = (M, x, y) \in L_c$, and $\pi \in \{0,1\}^*$, V_{cert} runs in time at most $g_V(n + |q|)$;*
- Completeness by a Relatively Efficient Prover: *For every $c, d \in \mathbb{N}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for every $n \in \mathbb{N}$ and every $q = (M, x, y) \in L_c$ such that $|q| \leq n^d$,*

$$\Pr[\pi \leftarrow P_{\mathsf{cert}}(c, 1^n, q) : V_{\mathsf{cert}}(c, 1^n, q, \pi) = 1] \geq 1 - \mathsf{negl}(n).$$

  Furthermore, P_{cert} on input $(c, 1^n, q)$ outputs a certificate of length $\ell(n)$ in time bounded by $g_P(n + |M| + T_M(x))$.
- Soundness: *For every $c \in N$, and every PPT P^*, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for every $n \in \mathbb{N}$,*

$$\Pr[(q, \pi) \leftarrow P^*(c, 1^n) : V_{\mathsf{cert}}(c, 1^n, q, \pi) = 1 \wedge q \notin L_c] \leq \mathsf{negl}(n).$$

*On the Existence of **P**-certificates.* In the plain model, a candidate construction of uniformly computationally-sound **P**-certificate systems come from Micali's CS-proofs [Mic00]. These constructs provide short certificates even for all of **NEXP**. However, since we here restrict to certificates only for **P**, the assumption that these constructions are sound **P**-certificates is falsifiable [Nao03]: Roughly speaking, we can efficiently test if an attacker outputs a valid proof of an incorrect statement, since whether a statement is correct or not can be checked in deterministic polynomial time.

2.5 Incomputable and Incompressible Functions

Definition 8 (Incomputable Function [AASY16]). *A function $\psi : \{0,1\}^n \to \{0,1\}^m$ is* incomputable *by a function class $\mathcal{C}$ if ψ is not contained in $\mathcal{C}$. We say that f is ϵ-incomputable by $\mathcal{C}$ if for every function $C : \{0,1\}^n \to \{0,1\}^m$ in $\mathcal{C}$, $\Pr[C(x) = f(x)] \leq \frac{1}{2^m} + \epsilon$ for uniform random $x \leftarrow \{0,1\}^n$.*

Definition 9 (Incompressible Function [DI06]). *A function $f : \{0,1\}^n \to \{0,1\}^m$ is* incompressible *by a function $C : \{0,1\}^n \to \{0,1\}^\ell$ if for every function $D : \{0,1\}^\ell \to \{0,1\}^m$, there exists $x \in \{0,1\}^n$ such that $D(C(x)) \neq f(x)$. We say that f is ϵ-incompressible by C if for every function $D : \{0,1\}^\ell \to \{0,1\}^m$, $\Pr[D(C(x)) = f(x)] \leq \frac{1}{2^m} + \epsilon$ for uniform random $x \leftarrow \{0,1\}^n$. We say that f is ℓ-incompressible (resp. (ℓ, ϵ)-incompressible) by a class $\mathcal{C}$ if for every $C : \{0,1\}^n \to \{0,1\}^\ell$ in $\mathcal{C}$, f is incompressible (resp. ϵ-incompressible) by C.*

Definition 10 (Non-deterministic Circuits and NP Circuits [AASY16]). *A* non-deterministic *circuit C has additional "non-deterministic input wires." We say that the circuit C evaluates to 1 on x if and only if there exists an assignment to the non-deterministic wires that makes C output 1 on x. An oracle circuit $C^{(\cdot)}$ is a circuit which in addition to the standard gates uses an additional gate (potentially with large fan-in). When instantiated with specific boolean function A, C^A is the circuit in which the additional gate is A. Given boolean function $A(x)$, an A-circuit is a circuit that is allowed to use A gates in addition to the standard gates. An* **NP***-circuit is a SAT-circuit (where SAT is the satisfiability function).*

The size of all circuits is the total number of wires and gates.

We now present commonly used assumptions in the derandomization literature to *explicitly* construct pseudorandom generators. [BFNW93, NW94, STV01, KVM02, SU06, SU09, FL97, MV05, TV00, SU05, GW02, GSTS03, BOV07, Dru13]:

Assumption 2 (E is hard for exponential size X-circuits) *There exists a problem $\mathbf{L}$ in $\mathbf{E} = \mathbf{DTIME}(2^{O(n)})$ and a constant $\beta > 0$, such that for every sufficiently large n, X-circuits of size $2^{\beta n}$ fail to compute the characteristic function of $\mathbf{L}$ on inputs of length n, where $X \in \{non\text{-}deterministic, co\text{-}non\text{-}deterministic, \mathbf{NP}\}$.*

Theorem 2 (Theorem 1.3, 1.10 [AASY16]). *If $\mathbf{E}$ is hard for exponential size X-circuits, where $X \in \{non\text{-}deterministic, co\text{-}non\text{-}deterministic, \mathbf{NP}\}$ (Assumption 2), then for every constant $c > 1$ there exists a constant $a > 1$ such that for every sufficiently large n, and every r such that $a \log n \leq r \leq n$ there is a function $\psi : \{0,1\}^r \to \{0,1\}$ that is n^{-c}-incomputable for size n^c X-circuits, Furthermore, ψ is computable in time $\mathrm{poly}(n^c)$ (or $\mathrm{poly}(n)$).*

2.6 NIZK without CRS Against Uniform Adversaries

We next define NIZK without CRS against uniform adversaries and NIWI.

Definition 11 (Non-Interactive Zero Knowledge [Sah99]). *$\Pi = (\mathsf{P}, \mathsf{V}, \mathsf{Sim})$ is an efficient single-theorem non-interactive zero knowledge proof system with soundness against uniform $T_{\mathsf{sound}}(n)$-time adversaries and zero-knowledge against non-uniform $T_{ZK}(n)$-time adversaries for language $L \in \mathsf{NP}$ with witness relation W, if the following are true:*

- *Completeness: For all $x \in L$, and all w such that $W(x,w) = 1$, we have $\mathsf{V}(x, \mathsf{P}(x,w))) = 1$*
- *Soundness against $T_{\mathsf{sound}}(n)$: For all uniform adversaries A running in time $T_{\mathsf{sound}}(n)$, $\Pr[\mathsf{V}(x,\pi) = 1] \leq \mathsf{negl}(n)$. Where, $(x,\pi) \leftarrow A(1^n)$ and $x \notin L$.*
- *Single-Theorem Zero Knowledge against $T_{ZK}(n)$: For all non-uniform $T_{ZK}(n)$-time adversaries $A = (A_1, A_2)$ we have that*

$$|\Pr[\mathsf{Expt}_A(n) = 1] - \Pr[\mathsf{Expt}_A^{\mathsf{Sim}}(n) = 1]| \leq \mathsf{negl}(n)$$

for following experiments $\mathsf{Expt}_A(n)$ and $\mathsf{Expt}_A^{\mathsf{Sim}}(n)$, where Sim is PPT and receives td as non-uniform advice.

```
Expt_A(n):                          Expt_A^Sim(n):

(x, w, κ) ← A_1(1^n)                (x, w, κ) ← A_1(1^n)
π ← P(x, w)                         π ← Sim(x, td)
return A_2(π, κ)                    return A_2(π, κ)
```

We now also define *witness indistinguishablity* as additional property of a proof system Π.

Definition 12 (Witness Indistinguishability against $T_{\mathsf{WI}}(n)$-time adversaries). *Let Π be a non-interactive proof system with prover P and verifier V for language $L \in \mathsf{NP}$ and witness relation $W : \{0,1\}^* \to \{0,1\}^*$. We say Π is* witness indistinguishable *if $\forall$ non-uniform $T_{\mathsf{WI}}(n)$-time verifier V^* and $\forall x \in L$, and $\forall w, w'$ such that $W(x, w) = W(x, w') = 1$, the view of V^* when interacting with $\mathsf{P}(x, w)$ is computationally indistinguishable from its view when interacting with $\mathsf{P}(x, w')$.*

In the remainder of this section, we focus on instantiations of the above primitives.

Theorem 3 ([BOV07]). *Assume that $\mathbf{E}$ is hard for exponential size co-non-deterministic circuits and that (subexponentially secure) trapdoor permutations (resp. one-way functions) exist. Then every language in $\mathbf{NP}$ has a (sub-exponentially indistinguishable) NIWI proof system (resp. non-interactive commitment scheme).*

Moreover, by correctly setting the output length of the commitment scheme in terms of the security parameter n, we obtain a non-interactive perfectly binding and computationally hiding commitment scheme, such that given a commitment c, the committed message (i.e., $\mathsf{val}(c)$) can be computed by a 2^{n^ϵ}-time algorithm, where n is the security parameter and ϵ is some constant.

To go from NIWI to NIZK, one can apply the well-known FLS technique [FLS99]. The simulator is provided with a trapdoor via non-uniform advice, which is not known to the uniform adversary in the real world. Note that we choose the trapdoor such that it *can* be obtained by a uniform adversary running in super-polynomial (sub-exponential) time. Formally, [BP04] show how to construct NIZK without CRS against uniform adversaries under the following assumptions:

Assumption A: There exists a NIWI proof system for every language $L \in \mathbf{NP}$ with WI against sub-exponential adversaries.

Assumption B: There exists a non-interactive perfectly binding and computationally hiding commitment scheme, such that given a commitment, the message can be computed by a 2^{n^ϵ}-time algorithm, where n is the security parameter and ϵ is some constant.

Assumption C: There exists a language $\Delta \in P$ and constants $\epsilon_1 < \epsilon_2 < 1$ such that:
  Δ is hard to sample in time $2^{n^{\epsilon_1}}$: For every probabilistic $2^{n^{\epsilon_1}}$-time algorithm A, the probability that $A(1^n) \in \Delta \cap \{0,1\}^n$ is negligible.
  Δ is easy to sample in time $2^{n^{\epsilon_2}}$: There exists a $2^{n^{\epsilon_2}}$ algorithm S_Δ such that for every $n \in N$, $\Pr[S_\Delta(1^n) \in \Delta \cap \{0,1\}^n] = 1$.

Theorem 4 ([BP04]). *Under Assumptions A, B and C, there exists a NIZK argument system without CRS for $\mathbf{NP}$ with soundness against sub-exponential uniform adversaries and zero-knowledge against sub-exponential adversaries.*

Lemma 1. *If $\mathbf{E}$ is hard for exponential size non-deterministc circuits and $\mathbf{P}$-cert with soundness against sub-exponential adversaries exists, then Assumption C is true.*

Proof (Sketch.). The assumption that $\mathbf{E}$ is hard for exponential size nondeterministc circuits implies the existence of a function ψ'' that has input length $c_1 \cdot \log(n)$, can be computed in time $O(n^{c_2})$ and no non-deterministic circuit of size n^{c_3} can compute ψ'' with better than $1/2 + 1/n^{c_3}$-probability.

Let Δ be the following language: $x = (x', \pi) \in \Delta$ if $\psi''(x') = 1$ and π is a valid **P**-cert proving that $\psi''(x') = 0$.

We first show that $\Delta \neq \emptyset$.

Assume $\Delta = \emptyset$, then to compute $\psi''(x')$, it would be sufficient to non-deterministically check whether there exists a valid **P**-certificate for x'. But since x' has length $O(\log n)$, **P**-cert has fixed polynomial length n^{c_4}, the verifier of the **P**-cert runs in fixed polynomial time n^{c_5}. By appropriately setting parameters so that $c_5 \leq c_3$, we obtain a non-deterministic circuit of size at most n^{c_3} that computes ψ'', leading to contradiction.

Finally, Δ is hard to sample in sub-exponential time $2^{n^{\epsilon_1}}$, due to the soundness of the **P**-cert. Moreover, padding the statements in the language appropriately (i.e. statements are now of the form $(x', \pi)\|0^\ell$, for appropriate choice of $\ell \in \mathrm{poly}(n)$, allows us to do a brute force search over the length of the input (x', π) to find $(x', \pi)\|0^\ell \in \Delta$ in time $2^{n^{\epsilon_2}}$.

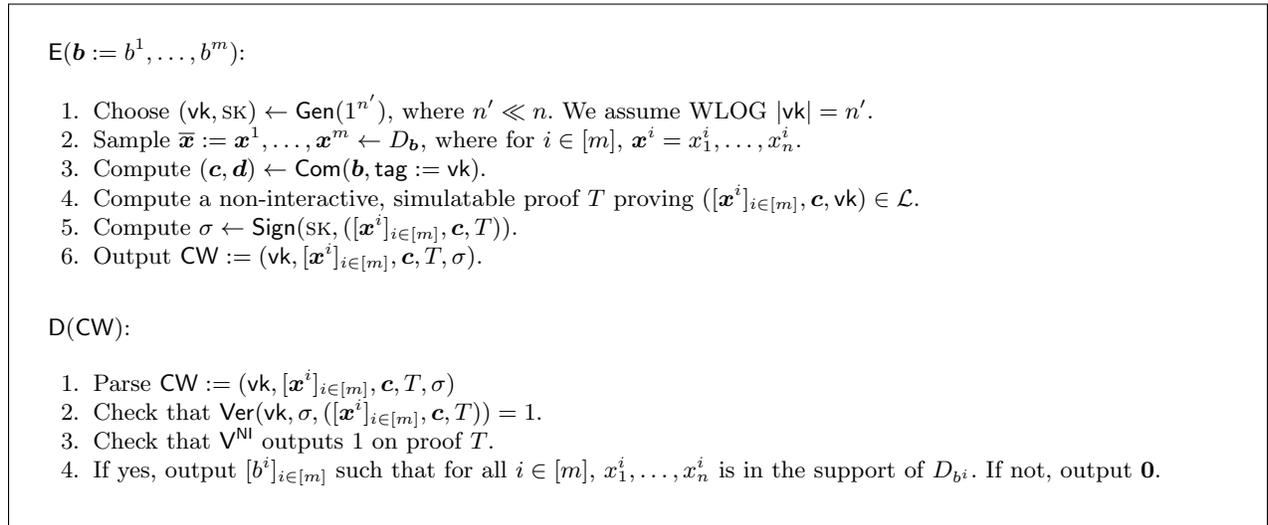**Corollary 1.** *Assuming that* **E** *is hard for exponential size (co-)non-deterministic circuits, the existence of sub-exponential trapdoor permutations, and the existence of* **P**-cert *with soundness against sub-exponential adversaries, there exists a NIZK argument system* without *CRS for* **NP** *with soundness against sub-exponential uniform adversaries and zero knowledge against sub-exponential adversaries.*

3 Construction for Multi-Bit Messages

Let $\mathcal{C} = (\mathsf{Com}, \mathsf{Open})$ be a tag-based, non-interactive commitment scheme that is perfectly binding (see Definition 2.3). Let $\Pi^{\mathsf{NI}} = (\mathsf{P}^{\mathsf{NI}}, \mathsf{V}^{\mathsf{NI}}, \mathsf{Sim}^{\mathsf{NI}})$ be a non-interactive simulatable proof system. Let $\mathcal{S} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ be a one-time signature scheme. Let D_0, D_1 be disjoint distributions over $\{0,1\}^n$. For $\boldsymbol{b} := b^1, \ldots, b^m \in \{0,1\}^m$, $D_{\boldsymbol{b}}$ denotes a draw from the product distribution $(D_{b^1}, \ldots, D_{b^m})$. We define the following language:

Language $\mathcal{L}$: $s := ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, \mathsf{tag}) \in \mathcal{L}$ iff $\exists \boldsymbol{b} := b^1, \ldots, b^m \in \{0,1\}^m$ such that for $i \in [m]$, $\boldsymbol{x}^i = (x_1^i, \ldots, x_n^i)$ is in the support of D_{b^i} and $\boldsymbol{c}$ is a commitment to $\boldsymbol{b}$ under tag.

The construction is presented in Figure 2:

$\mathsf{E}(\boldsymbol{b} := b^1, \ldots, b^m)$:

1. Choose $(\mathsf{vk}, \mathrm{SK}) \leftarrow \mathsf{Gen}(1^{n'})$, where $n' \ll n$. We assume WLOG $|\mathsf{vk}| = n'$.
2. Sample $\overline{\boldsymbol{x}} := \boldsymbol{x}^1, \ldots, \boldsymbol{x}^m \leftarrow D_{\boldsymbol{b}}$, where for $i \in [m]$, $\boldsymbol{x}^i = x_1^i, \ldots, x_n^i$.
3. Compute $(\boldsymbol{c}, \boldsymbol{d}) \leftarrow \mathsf{Com}(\boldsymbol{b}, \mathsf{tag} := \mathsf{vk})$.
4. Compute a non-interactive, simulatable proof T proving $([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, \mathsf{vk}) \in \mathcal{L}$.
5. Compute $\sigma \leftarrow \mathsf{Sign}(\mathrm{SK}, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T))$.
6. Output $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma)$.

$\mathsf{D}(\mathsf{CW})$:

1. Parse $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma)$
2. Check that $\mathsf{Ver}(\mathsf{vk}, \sigma, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T)) = 1$.
3. Check that V^{NI} outputs 1 on proof T.
4. If yes, output $[b^i]_{i \in [m]}$ such that for all $i \in [m]$, $x_1^i, \ldots, x_n^i$ is in the support of D_{b^i}. If not, output $\boldsymbol{0}$.

Fig. 2. Non-malleable code (E, D), secure against $\mathcal{F}$ tampering.

$\mathsf{E}_1(\mathsf{td}, \boldsymbol{b} := b^1, \ldots, b^m)$:

1. Choose $(\mathsf{vk}, \mathrm{SK}) \leftarrow \mathsf{Gen}(1^{n'})$
2. Sample $\overline{\boldsymbol{x}} := \boldsymbol{x}^1, \ldots, \boldsymbol{x}^m \leftarrow D_b$, where for $i \in [m]$, $\boldsymbol{x}^i = x_1^i, \ldots, x_n^i$.
3. Compute $(\boldsymbol{c}, \boldsymbol{d}) \leftarrow \mathsf{Com}(\boldsymbol{b}, \mathsf{tag} := \mathsf{vk})$.
4. <u>Simulate, using td, a non-interactive proof T' proving $s := ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, \mathsf{vk}) \in \mathcal{L}$.</u>
5. Compute $\sigma \leftarrow \mathsf{Sign}(\mathrm{SK}, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T'))$.
6. Output $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T', \sigma)$.

Fig. 3. ENCODING ALGORITHM WITH SIMULATED PROOF.

$\mathsf{E}_2(\mathsf{td}, \boldsymbol{b} := b^1, \ldots, b^m)$:

1. Choose $(\mathsf{vk}, \mathrm{SK}) \leftarrow \mathsf{Gen}(1^{n'})$
2. Sample $\overline{\boldsymbol{x}} := \boldsymbol{x}^1, \ldots, \boldsymbol{x}^m \leftarrow D_b$, where for $i \in [m]$, $\boldsymbol{x}^i = x_1^i, \ldots, x_n^i$.
3. <u>Compute $(\boldsymbol{c}', \boldsymbol{d}') \leftarrow \mathsf{Com}(\boldsymbol{0}, \mathsf{tag} := \mathsf{vk})$.</u>
4. Simulate, using td, a non-interactive proof T' proving $s := ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}', \mathsf{vk}) \in \mathcal{L}$.
5. Compute $\sigma \leftarrow \mathsf{Sign}(\mathrm{SK}, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}', T'))$.
6. Output $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}', T', \sigma)$.

Fig. 4. ENCODING ALGORITHM WITH SIMULATED PROOF AND COMMITMENTS.

$\mathsf{D}'(\mathsf{CW}) := \mathsf{D}_2'(\mathsf{D}_1'(\mathsf{CW}))$:

$\mathsf{D}_1'(\mathsf{CW})$:

1. Parse $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma)$
2. Check that $\mathsf{Ver}(\mathsf{vk}, \sigma, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T)) = 1$.
3. Check that V^{NI} outputs 1 on proof T
4. If not, output $\perp$, where $\perp$ is a special symbol.
5. If yes, output $(\boldsymbol{c}, \mathsf{tag} := \mathsf{vk})$.

$\mathsf{D}_2'(\boldsymbol{c}, \mathsf{tag} := \mathsf{vk})$:

1. If $\boldsymbol{c} = \perp$, output $[0]_{i \in [m]}$ and terminate.
2. Otherwise, check if there exists a string $\boldsymbol{d}$ and a string $\widetilde{\boldsymbol{b}}$ such that $\mathsf{Open}(\boldsymbol{d}, \boldsymbol{c}, \mathsf{vk}, \widetilde{\boldsymbol{b}}) = 1$. If yes, output $\widetilde{\boldsymbol{b}}$. Otherwise, output $[0]_{i \in [m]}$.

Fig. 5. ALTERNATE DECODING PROCEDURE D'.

$g(\mathsf{CW}, \mathsf{CW}^*)$:

1. Parse $\mathsf{CW} = (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma)$, $\mathsf{CW}^* = (\mathsf{vk}^*, [\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*, \sigma^*)$.
2. If $\mathsf{vk} = \mathsf{vk}^*$ and $\mathsf{Ver}(\mathsf{vk}^*, \sigma^*, ([\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*)) = 1$ then output 1. Otherwise output 0.

Fig. 6. THE PREDICATE $g(\mathsf{CW}, \mathsf{CW}^*)$.

Let $\Psi(p, x, y, z)$ be defined as a function that takes as input a predicate p, and variables x, y, z. If $p(x, y) = 1$, then Ψ outputs the m-bit string $\mathbf{0}$. Otherwise, Ψ outputs z.

Theorem 5. *Let* (E, D), E_1, E_2, D' *and* g *be as defined in Figures* 2, 3, 4, 5 *and* 6. *Let* $\mathcal{F}$ *be a computational class. If, for every pair of m-bit messages* $\boldsymbol{b}_0, \boldsymbol{b}_1$ *and for every tampering function* $f \in \mathcal{F}$, *all of the following hold:*

– **Simulation of proofs.**

1. $\Pr[g(\mathsf{CW}_0, f(\mathsf{CW}_0)) = 1] \overset{\mathsf{negl}(n)}{\approx} \Pr[g(\mathsf{CW}_1, f(\mathsf{CW}_1)) = 1]$,

2. $\Psi(g, \mathsf{CW}_0, f(\mathsf{CW}_0), \mathsf{D}(f(\mathsf{CW}_0))) \overset{PPT, \mathsf{negl}(n)}{\approx} \Psi(g, \mathsf{CW}_1, f(\mathsf{CW}_1), \mathsf{D}(f(\mathsf{CW}_1)))$,

where $f \in \mathcal{F}$, $\mathsf{CW}_0 \leftarrow \mathsf{E}(\boldsymbol{b}_0)$ and $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, \boldsymbol{b}_0)$.

– **Simulation of Commitments.**

1. $\Pr[g(\mathsf{CW}_1, f(\mathsf{CW}_1)) = 1] \overset{\mathsf{negl}(n)}{\approx} \Pr[g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 1]$,

2. $\Psi(g, \mathsf{CW}_1, f(\mathsf{CW}_1), \mathsf{D}(f(\mathsf{CW}_1))) \overset{PPT, \mathsf{negl}(n)}{\approx} \Psi(g, \mathsf{CW}_2, f(\mathsf{CW}_2), \mathsf{D}(f(\mathsf{CW}_2)))$,

where $f \in \mathcal{F}$, $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, \boldsymbol{b}_0)$ and $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$.

– **Simulation Soundness.**

$$\Pr[\mathsf{D}(f(\mathsf{CW}_2)) \neq \mathsf{D}'(f(\mathsf{CW}_2)) \wedge g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 0] \in O(1/n^c),$$

where $f \in \mathcal{F}$, $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$.

– **Hardness of $D_{\boldsymbol{b}}$ relative to Alternate Decoding.**

1. $\Pr[g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 1] \overset{PPT, O(1/n^c)}{\approx} \Pr[g(\mathsf{CW}_3, f(\mathsf{CW}_3)) = 1]$,

2. *For every Boolean function, represented by a circuit F over m variables,*

$$F \circ \mathsf{D}'(f(\mathsf{CW}_2)) \overset{stat, O(1/n^c)}{\approx} F \circ \mathsf{D}'(f(\mathsf{CW}_3)),$$

where $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$, and $\mathsf{CW}_3 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_1)$.

Then the construction presented in Figure 2 is a $O(1/n^c)$-non-malleable code for class $\mathcal{F}$.

We present the proof of Theorem 5 in Section 4.

4 Generic Analysis

In this section, we prove Theorem 5.

Fix $\boldsymbol{b} \in \{0, 1\}^m$. We take g to be the predicate that is used in the $\mathbf{MediumNM}^f_{\boldsymbol{b},g}(n)$ tampering experiment. Let $\mathsf{CW} \leftarrow \mathsf{E}(\boldsymbol{b})$. We must show that for every $f \in \mathcal{F} \subset \mathsf{P}$,

$$\Pr[g(\mathsf{CW}, f(\mathsf{CW})) = 1] \wedge \mathsf{D}(f(\mathsf{CW})) \neq \boldsymbol{b}] \leq \mathsf{negl}(n).$$

Let $\mathsf{CW} := (\mathsf{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma)$ and let $f(\mathsf{CW}) := (\mathsf{vk}^*, [\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*, \sigma^*)$. If $g(\mathsf{CW}, f(\mathsf{CW})) = 1$, it means that $\mathsf{vk} = \mathsf{vk}^*$ and $\mathsf{Ver}(\mathsf{vk}^*, \sigma^*, ([\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*)) = 1$ On the other hand, if $\mathsf{D}(f(\mathsf{CW})) \neq \boldsymbol{b}$, it must mean that $([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T) \neq ([\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*)$ But in this case we obtain a PPT adversary A that sees a single signature (σ) on message message $([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T)$ under verification key vk and produces a valid signature σ^* on message $([\boldsymbol{x}^{*i}]_{i \in [m]}, \boldsymbol{c}^*, T^*) \neq ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T)$ under challenge verification key vk, thus leading to a contradiction to the security of the one-time signature scheme $\mathcal{S}$.

Next, we must show that for any $\boldsymbol{b}_0, \boldsymbol{b}_1$ and any tampering function $f \in \mathcal{F}$, $\{\mathbf{MediumNM}^f_{\boldsymbol{b}_0,g}\}_{n \in \mathbb{N}} \overset{PPT, O(1/n^c)}{\approx} \{\mathbf{MediumNM}^f_{\boldsymbol{b}_1,g}\}_{n \in \mathbb{N}}$

To do so we consider the following hybrid argument:

Hybrid 0: The real game, $\mathbf{MediumNM}^f_{b_0,g}$, where the real encoding $\mathsf{CW}_0 \leftarrow \mathsf{E}(b_0)$ and the real decoding oracle D are used.

Hybrid 1: Replace the encoding from the previous game with $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, b_0)$.

Hybrid 2: Replace the encoding from the previous game with $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, b_0)$.

Hybrid 3: Replace the decoding from the previous game, with $\mathsf{D}'(f(\mathsf{CW}_2))$.

Hybrid 4: Same as Hybrid 3, but replace the encoding with $\mathsf{CW}_3 \leftarrow \mathsf{E}_2(\mathsf{td}, b_1)$.

The proofs of indistinguishability of consecutive hybrids follow identically to [BDKM18].

5 Multi-Bit NMC Against Bounded Poly Adversaries

We describe the underlying components required to instantiate the generic construction. The tampering class $\mathcal{F}$ corresponds to (uniform) tampering functions that run in time $O(n^{c_A})$, where n is security parameter. The length of the encoding is $L := O(n^{c_\ell})$, for some fixed constant c_ℓ. Therefore, the tampering function is allowed to run in time L^{c_A/c_ℓ} with respect to the input length L.

Let n be the input length for the hard distribution described in Section 5.1. We fix polynomials $t_\psi(n) = n^{c_\psi}$, $t_{\mathsf{com}}(n) = n^{c_{\mathsf{com}}}$ where c_ψ, c_{com} are constants (both greater than c_A) and superpolynomial time bounds $T_{\mathsf{com}}(n)$, $T'_{NIZK}(n)$, $T_{ZK}(n)$. such that

- $c_\psi \ll c_{\mathsf{com}}$,
- $T'_{NIZK}(n) \ll T_{\mathsf{com}}(n)$,
- $T_{ZK}(n)$ is subexponential.

The distribution described in Section 5.1 is hard for $t_\psi(n)$-time adversaries. $m \cdot \lambda \ll n$ is the length of the m-bit commitment using the commitment scheme described in Section 5.2, n is set such that $m \cdot \lambda + n' \leq (m+1) \cdot \lambda \in o(n)$ (so n is asymptotically larger than the length of the commitment–$m \cdot \lambda$–plus the length of the tag–n'.). These commitments are hiding for polynomial-time adversaries and quasi-non-malleable for adversaries in $\mathbf{BPtime}(T_{\mathsf{com}}(n)) \bigcap \mathbf{SIZE}(t_{\mathsf{com}}(n))$. The the non-interactive simulatable proof system in Section 5.3 has soundness against uniform, poly-time adversaries and zero knowledge against $T_{ZK}(n)$ time adversaries.

5.1 The Hard Distribution D_b (instance length n, hard against $t_\psi(n)$-time adversaries)

The following theorem is from [AASY16]:

Theorem 6. *If E is hard for exponential size nondeterministic circuits, then for every constant $c_\psi > 1$, there exists a constant $d > 1$ such that for every sufficiently large n, there is a function $\psi : \{0,1\}^n \to \{0,1\}$ that is (ℓ, n^{-c_ψ})-incompressible for size n^{c_ψ} circuits, where $\ell = n - d \cdot \log n$. Furthermore, ψ is computable in time $\mathrm{poly}(n^{c_\psi}) \in O(n^{c_{\mathsf{com}}})$.*

Setting parameters n, c_ψ, d as above, we let D_b be the uniform distribution over $\boldsymbol{x} \leftarrow \{0,1\}^n$, conditioned on $\psi(\boldsymbol{x}) = b$. The theorem above immediately implies the following:

Claim. Let n, c_ψ, d, ψ be as above, let $\widetilde{F}$ be any Boolean function over $(m+1) \cdot \lambda \leq n - d \cdot \log n < (1-\alpha)n$ variables, and let C be a size n^{c_ψ} circuit with input length n and output length m. Then, over random choice of $x \leftarrow \{0,1\}^n$, $\widetilde{F} \circ C(x)$ has correlation at most $1/n^{-c_\psi}$ with $\psi(x)$.

5.2 Commitment scheme $\mathcal{C} = (\mathsf{Com}, \mathsf{Open})$ (length $\lambda \ll n$, hiding for poly-time adversaries, and quasi non-malleable against adversaries in $\mathbf{BPtime}(T_{\mathsf{com}}(n)) \bigcap \mathbf{SIZE}(t_{\mathsf{com}}(n))$)

We instantiate the commitment scheme $\mathcal{C} = (\mathsf{Com}, \mathsf{Open})$ with the scheme presented in Section 7. Recall that the scheme has the following properties:

- Non-interactive with no-CRS.
- Perfectly binding,
- Quasi-non-malleable against in $\mathbf{BPtime}(T_{\mathsf{com}}(n)) \bigcap \mathbf{SIZE}(t_{\mathsf{com}}(n))$.

5.3 Non-Interactive Simulatable Proof System (Sound against uniform ppt adversaries, ZK against adversaries running in time $T_{ZK}(n)$)

Let $\Pi = (\mathsf{P}, \mathsf{V}, \mathsf{Sim})$ be a NIZK proof system for NP with no CRS (Construction given in Section 2.6) with soundness against uniform adversaries running in time $T_{NIZK}(n)$. We additionally require that the trapdoor can be extracted by uniform adversaries running in time $T'_{NIZK}(n)$.

Let $\mathcal{C}' = (\mathsf{Com}', \mathsf{Open}')$ be a non-interactive, perfectly binding, commitment scheme with no CRS that can be extracted in time $T_{NIZK}(n)$ and is hiding against adversaries running in time $T_{ZK}(n)$.

We also assume the existence of **P**-certificates with soundness against adversaries running in time $T_{NIZK}(n)$.

We define the proof system $\Pi^{\mathsf{NI}} = (\mathsf{P}^{\mathsf{NI}}, \mathsf{V}^{\mathsf{NI}}, \mathsf{Sim}^{\mathsf{NI}})$ for language $\mathcal{L}$ defined in Section 3 as follows:

P^{NI}: Recall that a witness w for statement $s := ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, \mathsf{tag}) \in \mathcal{L}$ consists of a string $\boldsymbol{b} = b^1, \ldots, b^m$ and an opening $\boldsymbol{d}$ such that (1) $\mathsf{Open}(\boldsymbol{c}, \boldsymbol{b}, \mathsf{tag}) = 1$ and (2) for all $i \in [m]$, $\psi(\boldsymbol{x}^i) = b^i$. Given a statement s and witness w, let P be a **P**-certificate that (1) and (2) hold.
Invoke P from proof system Π with the statement $s' = (s, \mathsf{com}) \in \mathcal{L}'$ using proof system Π, where $\mathcal{L}'$ is the language consisting of strings (s, com) such that com is a commitment to (w, P) and P is a **P**-certificate that (1) and (2) hold for (s, w). P outputs a proof π'. P^{NI} outputs proof $\pi = \mathsf{com} || \pi'$.

V^{NI}: On input statement s, proof π and language $\mathcal{L}$: Parse $\pi := \mathsf{com} || \pi'$. Run the underlying verifier V on π' for statement (s, com) and language $\mathcal{L}'$ and output whatever it does.

$\mathsf{Sim}^{\mathsf{NI}}$: On input (td, x), and language $\mathcal{L}$: Set com to a commitment to 0 and invoke the underlying Sim for Π with input $(\mathsf{td}, (s, \mathsf{com}))$ and language $\mathcal{L}'$.

Note that given the **P**-certificate P, computing the NIZK proof using Π^{NI} can be done in fixed polynomial time in the length of the statement (s, com). Moreover, given the trapdoor td, a simulated proof can also be computed in fixed polynomial time. The following claim is straightforward.

Claim. Given the above assumptions, $\Pi^{\mathsf{NI}} = (\mathsf{P}^{\mathsf{NI}}, \mathsf{V}^{\mathsf{NI}}, \mathsf{Sim}^{\mathsf{NI}})$ is a NIZK argument system for language $\mathcal{L}$ with zero knowledge against adversaries running in time $T_{ZK}(n)$ and trapdoor that can be extracted in time $T'_{NIZK}(n)$.

5.4 Main Theorem

Theorem 7. *For any constant $c_A > 1$, $\Pi = (\mathsf{E}, \mathsf{D})$ (presented in Figure 2) is a multi-bit, non-malleable code against (uniform) tampering functions that run in time $O(n^{c_A})$, if parameters $c_\psi, c_{\mathsf{com}}, T_{\mathsf{com}}(n), T'_{NIZK}(n), T_{ZK}(n)$ are chosen as described above and the underlying components are instantiated in the following way:*

- *For $b \in \{0, 1\}$, D_b is the distribution from Section 5.1.*
- *$\mathcal{C} := (\mathsf{Com}, \mathsf{Open})$ is the commitment scheme from Section 5.2.*
- *$\Pi^{\mathsf{NI}} := (\mathsf{P}^{\mathsf{NI}}, \mathsf{V}^{\mathsf{NI}}, \mathsf{Sim}^{\mathsf{NI}})$ the simulatable proof system from Section 5.3.*
- *$\mathcal{S} := (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ is any one-time signature scheme secure against PPT adversaries.*

Proof. To prove the theorem, we need to show that the necessary properties from Theorem 5 hold. We next go through these one by one.

Simulation of proofs.

1. $\Pr[g(\mathsf{CW}_0, f(\mathsf{CW}_0)) = 1] \overset{\mathsf{negl}(n)}{\approx} \Pr[g(\mathsf{CW}_1, f(\mathsf{CW}_1)) = 1],$

2. $\Psi(g, \mathsf{CW}_0, f(\mathsf{CW}_0), \mathsf{D}(f(\mathsf{CW}_0))) \overset{PPT,\mathsf{negl}(n)}{\approx} \Psi(g, \mathsf{CW}_1, f(\mathsf{CW}_1), \mathsf{D}(f(\mathsf{CW}_1))),$

where $f \in \mathcal{F}$, $\mathsf{CW}_0 \leftarrow \mathsf{E}(\boldsymbol{b}_0)$ and $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, \boldsymbol{b}_0)$.
This follows by ZK property of Π^{NI}.

Simulation of Commitment.

1. $\Pr[g(\mathsf{CW}_1, f(\mathsf{CW}_1)) = 1] \overset{\mathsf{negl}(n)}{\approx} \Pr[g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 1],$

2. $\Psi(g, \mathsf{CW}_1, f(\mathsf{CW}_1), \mathsf{D}(f(\mathsf{CW}_1))) \overset{PPT,\mathsf{negl}(n)}{\approx} \Psi(g, \mathsf{CW}_2, f(\mathsf{CW}_2), \mathsf{D}(f(\mathsf{CW}_2))),$

where $f \in \mathcal{F}$, $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, \boldsymbol{b}_0)$ and $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$.
This follows from hiding property of the commitment scheme $\mathcal{C}$.

Simulation Soundness.

$$\Pr_r[\mathsf{D}(f(\mathsf{CW}_2)) \neq \mathsf{D}'(f(\mathsf{CW}_2)) \wedge g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 0] \in O(1/n^{c_{\mathsf{com}}}),$$

where $f \in \mathcal{F}$, $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$.
We begin by defining the following:

$$P_0(n) := \Pr[\mathsf{D}(f(\mathsf{CW}_0)) \neq \mathsf{D}'(f(\mathsf{CW}_0)) \wedge g(\mathsf{CW}_0, f(\mathsf{CW}_0)) = 0],$$

where $f \in \mathcal{F}$, $\mathsf{CW}_0 \leftarrow \mathsf{E}(\boldsymbol{b}_0)$

$$P_1(n) := \Pr_r[\mathsf{D}(f(\mathsf{CW}_1)) \neq \mathsf{D}'(f(\mathsf{CW}_1)) \wedge g(\mathsf{CW}_1, f(\mathsf{CW}_1)) = 0],$$

where $f \in \mathcal{F}$, $\mathsf{CW}_1 \leftarrow \mathsf{E}_1(\mathsf{td}, \boldsymbol{b}_0)$

$$P_2(n) := \Pr_r[\mathsf{D}(f(\mathsf{CW}_2)) \neq \mathsf{D}'(f(\mathsf{CW}_2)) \wedge g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 0],$$

where $f \in \mathcal{F}$, $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$.
We prove the following sequence of claims, which immediately imply the simulation soundness property.

Claim. $P_0(n) \in \mathsf{negl}(n)$.

Since $\mathsf{D}(f(\mathsf{CW}_1)) \neq \mathsf{D}'(f(\mathsf{CW}_1))$ can only occur if the NIZK proof verifies, but the statement being proved is false, this follows from the soundness of the NIZK proof system Π^{NI}.

Claim. $|P_1(n) - P_0(n)| \in \mathsf{negl}(n)$.

This holds due to complexity leveraging–i.e. by appropriately setting parameters, one can check whether the statement being proved is true or false (by deciding whether $\boldsymbol{x}$ is in the support of D_0 or D_1 and by extracting from the commitment scheme) without distinguishing a real from simulated proof since $T_{ZK}(n)$ is subexponential.

Claim. $|P_2(n) - P_1(n)| \in O(1/n^{c_{\text{com}}})$.

Proof. Assume $|P_2(n) - P_1(n)| \notin O(1/n^{c_{\text{com}}})$, we will construct an adversary/distinguisher (A, D) in $\textbf{BPtime}(T_{\text{com}}(n)) \bigcap \textbf{SIZE}(t_{\text{com}}(n))$ that breaks the $O(1/n^{c_{\text{com}}})$-non-malleability of commitment scheme $\mathcal{C}$. Specifically, we must show an adversary A, distinguisher D in $\textbf{BPtime}(T_{\text{com}}(n)) \bigcap \textbf{SIZE}(t_{\text{com}}(n))$ such that D distinguishes the output of $\text{mim}_{\mathcal{C}}^A(\boldsymbol{b}_0)$ from $\text{mim}_{\mathcal{C}}^A(\boldsymbol{0})$ with advantage $a(n) \notin O(1/n^{c_{\text{com}}})$.

$A = (A_1, A_2)$ is specified as follows:

On input security parameter 1^n, A_1 does as follows:

- A_1 generates keys $(\text{vk}, \text{SK}) \leftarrow \text{Gen}(1^n)$
- A_1 runs in uniform time $T'_{NIZK}(n) \leq T_{\text{com}}(n)$ to recover the trapdoor td of the NIZK.
- A_1 outputs $\text{tag} := \text{vk}$ to its challenger as the desired tag and outputs td, SK to A_2.

On input $\text{td}, \text{SK}, \text{vk}, \boldsymbol{c}$, A_2 does as follows:

- For $i \in [m]$, sample $\boldsymbol{x}^i \sim D_{b^i}$ (in time $m \cdot \text{poly}(n^{c_\psi}) \in O(n^{c_{\text{com}}})$, where poly is a fixed polynomial.
- Use td to generate a simulated proof T in fixed polynomial time and compute $\sigma \leftarrow \text{Sign}(\text{SK}, ([\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T))$ in fixed polynomial time.
- Compute $f(\text{vk}, [\boldsymbol{x}^i]_{i \in [m]}, \boldsymbol{c}, T, \sigma) = [\text{vk}', \boldsymbol{x}'^i]_{i \in [m]}, \boldsymbol{c}', T', \sigma')$.
- If the predicate g evaluates to 1, the signature σ' or proof T does not verify, output $\perp$ (this computation takes fixed polynomial time).
- Otherwise, output $(\boldsymbol{c}', \text{out} := [\boldsymbol{x}'^i]_{i \in [m]})$. Note that in this case, $\text{vk}' \neq \text{vk}$ (corresponding to the tag of the commitment) since g evaluates to 0 and σ verifies.

Distinguisher D receives the committed value $\boldsymbol{v}' = v'_1, \ldots, v'_m$ underlying $\boldsymbol{c}'$ (or receives $\perp$) as well as out (the additional output of adversary A). D outputs 0 if for all $i \in [m]$, $v'_i = \psi(\boldsymbol{x}^i)$ (or if its input is $\perp$) and outputs 1 otherwise (computed in time $m \cdot \text{poly}(n^{c_\psi}) \in O(n^{c_{\text{com}}})$).

Clearly,

$$\Pr_{\boldsymbol{c} \leftarrow \text{Com}(\boldsymbol{b}_0, \text{vk})}[D(\boldsymbol{v}', \text{out}) = 1] = P_2(n)$$

and

$$\Pr_{\boldsymbol{c} \leftarrow \text{Com}(\boldsymbol{0}, \text{vk})}[D(\boldsymbol{v}', \text{out}) = 1] = P_1(n)$$

Thus, we have that

$$\left| \Pr_{\boldsymbol{c} \leftarrow \text{Com}(\boldsymbol{b}_0, \text{vk})}[D(\boldsymbol{v}', \text{out}) = 1] - \Pr_{\boldsymbol{c} \leftarrow \text{Com}(\boldsymbol{0}, \text{vk})}[D(\boldsymbol{v}', \text{out}) = 1] \right| \notin O(1/n^{c_{\text{com}}}).$$

Moreover, A, D are in $\textbf{BPtime}(T_{\text{com}}(n)) \bigcap \textbf{SIZE}(t_{\text{com}}(n))$. Thus, we obtain a contradiction to the $O(1/n^{c_{\text{com}}})$ non-malleability of the commitment scheme against adversaries, distinguishers in $\textbf{BPtime}(T_{\text{com}}(n)) \bigcap \textbf{SIZE}(t_{\text{com}}(n))$.

Hardness of D_b relative to Alternate Decoding.

1. $\Pr[g(\text{CW}_2, f(\text{CW}_2)) = 1] \overset{O(1/n^{c_\psi})}{\approx} \Pr[g(\text{CW}_3, f(\text{CW}_3)) = 1]$,

2. For every Boolean function, represented by a circuit F over m variables,

$$F \circ \text{D}'(f(\text{CW}_2)) \overset{stat, O(1/n^{c_\psi})}{\approx} F \circ \text{D}'(f(\text{CW}_3)),$$

where $f \in \mathcal{F}$, $\mathsf{CW}_2 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_0)$ and $\mathsf{CW}_3 \leftarrow \mathsf{E}_2(\mathsf{td}, \boldsymbol{b}_1)$.

We consider a sequence of distributions where we switch the internal random variables of E_2 from from $\boldsymbol{x}^i \leftarrow D_{b_0^i}$, for all $i \in [m]$ to $\boldsymbol{x}^i \leftarrow D_{b_1^i}$, for all $i \in [m]$. Namely, for each $i \in \{0, \ldots, m\}$ we consider a distribution where for $j \le i$, $\boldsymbol{x}^j \leftarrow D_{b_1^i}$ and for $j > i$, $\boldsymbol{x}^j \leftarrow D_{b_0^i}$.

We must show that (1) and (2) hold for each consecutive pair of distributions. When considering the i-th consecutive pair, fix all random variables except the i-th variable $\boldsymbol{X}^i$ to values $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}, \boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$. Let $\boldsymbol{X}^i$ be a random variable such that with probability $1/2$, $\boldsymbol{X}^i \leftarrow D_{b_0^i}$ and with probability $1/2$, $\boldsymbol{X}^i \leftarrow D_{b_1^i}$. $\boldsymbol{X}^i = \boldsymbol{X}^{i,\gamma}$ where $\gamma \leftarrow \{0, 1\}$, and let random variable CW^i denote the output of E_2 when using random variables $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}, \boldsymbol{X}^i, \boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$.

To show (1), assume $\Pr[g(\mathsf{CW}_2, f(\mathsf{CW}_2)) = 1]$ and $\Pr[g(\mathsf{CW}_3, f(\mathsf{CW}_3)) = 1]$ differ by $a(n) \notin O(1/n^{c_\psi})$. This implies that, for some $i \in [m]$, there is a circuit that takes as input $\boldsymbol{X}^i$, hardwires all other random variables, and outputs 1 in the case that $g(\mathsf{CW}^i, f(\mathsf{CW}^i)) = 1$ and 0 otherwise, implying that it has $a(n) \notin O(1/n^{c_\psi})$ correlation to $\psi(\boldsymbol{X}^i)$. We will show that the above can be computed by a circuit C of size n^{c_ψ} with input $\boldsymbol{X}^i$, thus contradicting Claim 5.1, which (as a special case) says that a circuit of size n^{c_ψ} has at most $O(1/(n^{c_\psi}))$ correlation with $\psi(\boldsymbol{X}^i)$. Details follow.

Given non-uniform advice td, f, we construct the distribution of circuits $\mathcal{C}_{f,\mathsf{td}}^1$. A draw $C \sim \mathcal{C}_{f,\mathsf{td}}^1$ is done as follows:

1. Sample signature keys $(\mathsf{vk}, \textsc{sk}) \leftarrow \mathsf{Gen}(1^n)$,
2. Sample random commitment to 0^m: $(\boldsymbol{c}', \boldsymbol{d}') \leftarrow \mathsf{Com}(0^m, \mathsf{tag} := \mathsf{vk})$,
3. Sample $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}$ from $D_{b_0^i}$, and $\boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$ from $D_{b_1^i}$.
4. Output the following circuit C that has the following structure:
   - **hardcoded variables:** f, $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}$, $\bar{c}'$, $[T_j'^{\beta,i}]_{\beta \in \{0,1\}, i \in [m], j \in [n]}$, $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}, \boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$.
   - **input:** $\boldsymbol{X}^i$.
   - **computes and outputs:**
$$g(\mathsf{CW}, f(\mathsf{CW}^i)).$$

Note that given all the hardwired variables, computing CW^i can be done in n^{c_ψ} time since it only requires computing the simulated proof T and signature σ, which can both be done in fixed polynomial time less than n^{c_ψ}. Additionally, f can be computed in time $n^{c_A} < n^{c_\psi}$. Finally, it can be seen that g can be computed in fixed polynomial time less than n^{c_ψ} (since it only involves comparison of strings and signature verification, both of which take fixed polynomial time in the length of the input). Thus, the entire circuit has size $O(n^{c_\psi})$.

To show (2), assume $\mathsf{D}'(f(\mathsf{CW}_2))$ and $\mathsf{D}'(f(\mathsf{CW}_3))$ have greater than $1/n^{c_\psi}$ statistical distance. This implies that there exists a distinguisher F (represented by an m-bit Boolean function) such that $F \circ \mathsf{D}'(f(\mathsf{CW}_2))$ is more than $1/n^{c_\psi}$-far from $F \circ \mathsf{D}'(f(\mathsf{CW}_3))$. This implies that, for some $i \in [m]$, the output of $F \circ \mathsf{D}'(f(\mathsf{CW}^i))$ is $a(n) \notin O(1/n^{c_\psi})$-correlated with $\psi(\boldsymbol{X}^i)$. Note that, by definition, $F \circ \mathsf{D}'(f(\mathsf{CW}^i)) = F \circ \mathsf{D}_2' \circ \mathsf{D}_1'(f(\mathsf{CW}^i))$, where D_1' has output length $(m+1) \cdot \lambda$ ($m \cdot \lambda$ for the size of the non-malleable commitment and λ for the length of the tag of the non-malleable commitment). We will show that $\mathsf{D}_1'(f(\mathsf{CW}^i))$ can be computed by a circuit C of size $O(n^{c_\psi})$ (drawn from some distribution $\mathcal{C}$ over circuits) with input $\boldsymbol{X}^i$. We then use Claim 5.1, which says that if C is a size $O(n^{c_\psi})$ circuit taking inputs of length n bits and producing outputs of length $(m+1) \cdot \lambda < (1-\alpha)n$-bits and and $\widetilde{F}$ is any $(m+1) \cdot \lambda < (1-\alpha)n$-bit input Boolean function then the output of $\widetilde{F}(C(\boldsymbol{X}^i))$ is at most $O(1/n^{c_\psi})$-correlated with $\psi(\boldsymbol{X}^i)$, instantiating $\widetilde{F} := F \circ \mathsf{D}_2'$. This yields a contradiction. Details follow.

Given non-uniform advice td, f, we construct the distribution of circuits $\mathcal{C}_{f,\mathsf{td}}^2$. A draw $C \sim \mathcal{C}_{f,\mathsf{td}}^2$ as follows:

1. Sample signature keys $(\mathsf{vk}, \textsc{sk}) \leftarrow \mathsf{Gen}(1^n)$,
2. Sample random commitment to 0^m: $(\boldsymbol{c}', \boldsymbol{d}') \leftarrow \mathsf{Com}(0^m, \mathsf{tag} := \mathsf{vk})$,
3. Sample $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}$ from $D_{b_0^i}$, and $\boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$ from $D_{b_1^i}$.

4. Output the following circuit C that has the following structure:
   - **hardcoded variables:** f, $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}$, $\overline{c}'$, $[T_j'^{\beta,i}]_{\beta \in \{0,1\}, i \in [m], j \in [n]}$, $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{i-1}, \boldsymbol{x}^{i+1}, \ldots, \boldsymbol{x}^m$.
   - **input:** $\boldsymbol{X}^i$.
   - **computes and outputs:**
$$\mathsf{D}_1'(f(\mathsf{CW}^i)).$$

Given all the hardwired variables, computing CW^i can be done in time $O(n^{c_\psi})$ since it only requires computing the simulated proof T and signature σ, which can both be done in fixed polynomial time less than n^{c_ψ}. Additionally, f can be computed in time $n^{c_A} < n^{c_\psi}$, and D_1' can be computed in fixed polynomial time less than n^{c_ψ}, since it only involves verifying the signature σ and proof T, which both take fixed polynomial time.

6 4-Tag Non-Malleable Commitment

Let $\mathcal{C}'' := (\mathsf{Com}'', \mathsf{Open}'')$ be a non-interactive, statistically binding commitment scheme for m-bit messages. Given security parameter $t \gg m$, Com'' has circuit size t and is hiding against adversaries running in time $2^{t^{\epsilon_5'}}$. Let ψ' be a function, which on input length ℓ can be computed in time 2^ℓ, but is $(1/2 + 1/\ell^{\epsilon_5})$-hard for NP circuits of size $2^{\epsilon_5 \cdot \ell}$.

Let c_4, c_3, c_2, c_1 be constants greater than 1 and let $\epsilon_1', \epsilon_2', \epsilon_3', \epsilon_4'$ be constants less than 1 such that:

$$\epsilon_5 \cdot c_4 > c_3, \epsilon_5 \cdot c_3 > c_2, \epsilon_5 \cdot c_2 > c_1 > c_{\mathsf{com}}.$$

$$\epsilon_5' \cdot \epsilon_1' > \epsilon_2', \epsilon_5' \epsilon_2' > \epsilon_3', \epsilon_5' \epsilon_3' > \epsilon_4'.$$

$\mathsf{Com}'(\mathsf{msg} \in \{0,1\}^m, \mathsf{tag} \in [4])$:

1. Choose $\mathsf{msg}^1, \mathsf{msg}^2$ at random, conditioned on $\mathsf{msg}^1 \oplus \mathsf{msg}^2 = \mathsf{msg}$.
2. Set $t := n^{\epsilon_{\mathsf{tag}}}$, $\ell := c_{\mathsf{tag}} \cdot \log n$.
3. For $i \in [m]$, sample $x_i \in \{0,1\}^\ell$, at random such that $\psi'(x_i) = \mathsf{msg}_i^1$.
4. Compute $(c, d) \leftarrow \mathsf{Com}''(\mathsf{msg}^2, t)$.
5. Output commitment $(c, [x_i]_{i \in [m]})$ and decommitment (msg^2, d).

$\mathsf{Open}'(\mathsf{msg}, (c, [x_i]_{i \in [m]}), (\mathsf{msg}^2, d))$:

1. Check that $\mathsf{Open}''(\mathsf{msg}^2, c, d) = 1$
2. For $i \in [m]$, let $\mathsf{msg}_i^1 := \psi'(x_i)$.
3. If $\mathsf{msg} = \mathsf{msg}^1 \oplus \mathsf{msg}^2$, output 1.
4. Otherwise, output 0.

Fig. 7. 4-TAG NON-MALLEABLE COMMITMENT $\mathcal{C}' = (\mathsf{Com}', \mathsf{Open}')$.

Theorem 8. *Given $\mathcal{C}''$ and ψ' as above, $\mathcal{C}'$ is a $O(1/n^{c_{\mathsf{com}}})$, 4-tag quasi-non-malleable commitment scheme against non-uniform adversaries of size $n^{c_{\mathsf{com}}}$ with commitment length that is a fixed polynomial. Moreover, ψ' and $\mathcal{C}''$ as above can be instantiated under the assumptions that $\mathbf{E}$ is hard for exponential size $\mathbf{NP}$-circuits (via Theorem 2) and that sub-exponential one-way functions exist (via Theorem 3).*

We show that $\mathcal{C}'$ has the required properties:

Hiding. Hiding of $\mathcal{C}'$ follows immediately from the hiding of the underlying commitment scheme $\mathcal{C}''$.

Statistically Binding. The binding property follows from the fact that ψ' is a function and the binding property of the underlying commitment scheme $\mathcal{C}''$.

Non-Malleability. One-to-one non-malleability against adversaries running in time $n^{\epsilon_5 \cdot c_1}$. Assume $\mathsf{tag} = i$ on the left and $\mathsf{tag} = j$ on the right, where $i, j \in [4]$ and $i \neq j$. The left commitment has parameters $t = n^{\epsilon'_i}$ and $\ell = c_i \cdot \log n$ and the right commitment has paramters $t = n^{\epsilon_j}$ and $\ell = c_j \cdot \log n$.

Case 1: $i < j$. In this case, $\epsilon'_5 \epsilon'_i > \epsilon'_j$. This means that we can extract the committed value from $(c, [x_i]_{i \in [m]})$ on the right in time $2^{n^{\epsilon'_j}}$ (using brute-force search and by evaluating ψ' in polynomial time), while the commitment c on the left is hiding against $2^{n^{\epsilon'_j}} < 2^{n^{\epsilon'_5 \cdot \epsilon'_i}}$-time adversaries.

Case 2: $i > j$. In this case, $\epsilon_5 c_i > c_j$. This means that we can extract the committed value from $(c, [x_i]_{i \in [m]})$ with NP-circuits of size n^{c_j} (by evaluating ψ' on $x_1, \ldots, x_m$ and extracting the committed value from c with NP-circuit of size $m \cdot n^{\epsilon'_j}$), while the value committed by $[x_i]_{i \in [m]}$ on the left is hiding against $n^{c_j} < n^{\epsilon_5 \cdot c_i}$-size NP circuits.

7 Tag Amplification

Let $\mathcal{C}_{i-1} := (\mathsf{Com}_{i-1}, \mathsf{Open}_{i-1})$ be a non-interactive, statistically binding commitment scheme for τ_{i-1}-tags. Let $\Pi = (\mathsf{P}, \mathsf{V}, \mathsf{Sim})$ be a NIZK argument system for language $\mathcal{L}_i$ with no CRS, soundness against uniform adversaries running in time $T_{NIZK,i-1}(n)$, with trapdoor that can be extracted in uniform time $T'_{NIZK,i-1}(n)$, and zero knowledge against subexponential adversaries. We construct commitment scheme $\mathcal{C}$ with $\tau_i := \binom{\tau_{i-1}}{2}$ number of tags. For convenience, we represent tags tag of the new commitment scheme as subsets of $[\tau_{i-1}]$ of size $\tau_{i-1}/2$. Note that there is an efficiently computable bijection between such tags and the set $[\binom{\tau_{i-1}}{2}]$.

$\mathcal{L}_i$: $\boldsymbol{c}' = (\boldsymbol{c}, \mathsf{com}) \in \mathcal{L}_i$ using proof system Π, where $\mathcal{L}_i$ is the language consisting of strings $(\boldsymbol{c}, \mathsf{com})$ such that com is a commitment to P and P is a **P**-certificate that $\boldsymbol{c} = (c_1, \ldots, c_{\tau_{i-1}/2})$ are all well-formed commitments under Com_{i-1} to the same message..

$\mathsf{Com}_i(\mathsf{msg} \in \{0,1\}^m, \mathsf{tag} \subseteq [\tau_{i-1}], |\mathsf{tag}| = \tau_{i-1}/2)$:

1. Let $\mathsf{tag}_1, \ldots, \mathsf{tag}_{\tau_{i-1}/2}$ be a lexicographical ordering of the set tag.
2. For $j \in [\tau_{i-1}/2]$, compute $(c_j, d_j) \leftarrow \mathsf{Com}_{i-1}(\mathsf{msg}, \mathsf{tag}_j)$.
3. Compute a proof π using proof system Π proving that all commitments commit to the same value.
4. Output commitment $(c_1, \ldots, c_{\tau_{i-1}/2}, \pi)$ and decommitment information $(d_1, \ldots, d_{\tau_{i-1}/2})$.

$\mathsf{Open}_i(\mathsf{msg}, (c_1, \ldots, c_{\tau_{i-1}/2}, \pi), (d_1, \ldots, d_{\tau_{i-1}/2}))$:

1. Verify the proof π. If the proof does not verify, output 0 and terminate.
2. For all $j \in [\tau_{i-1}/2]$, check that $\mathsf{Open}_{i-1}(\mathsf{msg}, c_j, d_j) = 1$.
3. If all check hold, output 1.
4. Otherwise, output 0.

Fig. 8. AMPLIFICATION FROM τ_{i-1}-TAG 1-1 NM COM TO $\tau_i := \binom{\tau_{i-1}}{2}$-TAG 1-1 NM COM.

Theorem 9. *Let N be subexponential in n. Assume the existence of primitives as described in Figure 8 such that for $i \in [\log^* N]$, $T_{NIZK,i-1}(n) \geq T'_{NIZK,i}(n) \gg T_{NIZK,i}(n)$. Let $\mathcal{C}_0$ be instantiated with $\mathcal{C}'$ from Section 6. Then $\mathcal{C}_{\log^* N}$ is a quasi-non-malleable commitment scheme with the following properties:*

- *The number of tags, $\tau_{\log^* N} = N$.*
- *It is hiding against non-uniform ppt adversaries.*

- *It is $O(1/n^{c_{\text{com}}})$-non-malleable against adversaries, distinguishers in $\mathbf{BPtime}(T_{NIZK,\log^* n}(n)) \bigcap \mathbf{SIZE}(t_{\log^* n}(n))$ (See Section 2.1 for the definition of this computational class), where $T_{NIZK,\log^* N}(n) = T_{\text{com}}(n)$ and $t_{\log^* N}(n) = t_{\text{com}}(n)$.*
- *It has commitments of fixed polynomial length. By appropriately setting the security parameter, we may assume the length is $\lambda \ll n$.*

In order to satisfy that for all $i \in [\log^* N]$, $T_{NIZK,i-1}(n) \geq T'_{NIZK,i}(n) \gg T_{NIZK,i}(n)$, we must obtain a "tower" of uniform languages $\Delta_1, \ldots, \Delta_{\log^* N}$ where for $i \in [\log^* N]$, Δ_i is hard to sample in time $T_{NIZK,i}(n)$ and easy to sample in time $T'_{NIZK,i}n$. Such a tower of (uniform) languages exists assuming that Assumption C holds (see Section 2.6), since existence of a single Δ with sub-exponential hardness is sufficient for constructing a tower of languages $\Delta_1, \ldots, \Delta_{\log^* N}$ of depth $\log^* N$. Moroever, **P**-cert with soundness against sub-exponential adversaries implies Assumption C (See the proof of Lemma 1 for more details). Thus, **P**-cert with soundness against sub-exponential adversaries implies a "tower" of languages as required above. Similar constructions of "towers" of assumptions in the *non-uniform* setting were established in [KS17b].

Proof. It is clear that $\mathcal{C}_{\log^* N}$ is a commitment scheme with N tags which is hiding against non-uniform ppt adversaries and has commitments of fixed polynomial length. We therefore proceed to prove that $\mathcal{C}_{\log^* N}$ is non-malleable.

First, we note that $\mathcal{C}_0$ with $\mathcal{C}'$ from Section 6, is non-malleable against adversaries, distinguishers in $\mathbf{SIZE}(t_0(n))$, where $t_0(n) = n^{c_{\text{com}}}$.

Next, we show that if $\mathcal{C}_{i-1}$ is a commitment scheme that is non-malleable against adversaries, distinguishers in $\mathbf{BPtime}(T_{NIZK,i-1}(n)) \bigcap \mathbf{SIZE}(t_{i-1}(n))$ then $\mathcal{C}_i$ is a commitment scheme that is non-malleable against adversaries, distinguishers in $\mathbf{BPtime}(T_{NIZK,i}(n)) \bigcap \mathbf{SIZE}(t_i(n))$ (where $t_{i-1}(n) - t_i(n) \in \text{poly}(n)$, for some fixed polynomial poly).

For compactness, we let $\mathcal{DA}_i$ denote the computational class $\mathbf{BPtime}(T_{NIZK,i}(n)) \bigcap \mathbf{SIZE}(t_i(n))$, for $i \in [\log^* N]$ and denote $\mathbf{SIZE}(t_0(n))$ for $i = 0$, in the remainder of the proof.

Recall that to prove non-malleability, we must show that for every pair of messages $\mathsf{msg}_0, \mathsf{msg}_1 \in \{0,1\}^m$ and any $A \in \mathcal{DA}_i$, $\mathsf{mim}_{\mathcal{C}_i}^A(\mathsf{msg}_0) \overset{\mathcal{DA}_i, O(1/n^{c_{\text{com}}})}{\approx} \mathsf{mim}_{\mathcal{C}_i}^A(\mathsf{msg}_1)$.

Towards proving this, we specify below a sequence of hybrid distributions $H_0, H_1, H_2, H_{2,0}, \ldots, H_{2,\tau_{i-1}/2}, H_3$. Recall that in each hybrid distribution, the adversary receives an input commitment of the form $(\mathsf{tag}, c_1, \ldots, c_{\tau_{i-1}/2}, \pi)$ and produces an output of the form $(\mathsf{tag}', c'_1, \ldots, c'_{\tau_{i-1}/2}, \pi')$, along with an output string out.

Random variables. We next introduce random variables that will be used in the analysis. For $\chi \in \{H_0, H_1, H_{2,0}, \ldots, H_{2,\tau_{i-1}/2}, H_2, H_3\}$, define random variable out^χ to be the string out outputted by the adversary in the corresponding hybrid.

For $\chi \in \{H_0, H_1, H_{2,0}, \ldots, H_{2,\tau_{i-1}/2}, H_2, H_3\}$, define random variable v_ℓ^χ to be $\perp$ if outputted proof π' does not verify in hybrid χ, and otherwise, to denote the value committed in the ℓ-th sub-commitment c'_ℓ, output by the adversary in hybrid χ.

For $\chi \in \{H_0, H_1, H_{2,0}, \ldots, H_{2,\tau_{i-1}/2}, H_2, H_3\}$, define random variable v_{diff}^χ to be $\perp$ if outputted proof π' does not verify in hybrid χ, and otherwise, to denote the value committed in the ℓ^*-th sub-commitment c'_{ℓ^*}, output by the adversary in hybrid χ, where ℓ^* is the lexicographically first index such that $\mathsf{tag}'_{\ell^*} \notin \mathsf{tag}$.

For $\chi \in \{H_0, H_3\}$, define random variable v_{com}^χ to be the value committed to in $(\mathsf{tag}', c'_1, \ldots, c'_{\tau_{i-1}/2}, \pi')$ output in Hybrid χ. Note that if π' does not verify, then v_{com}^χ must be set to $\perp$.

Hybrid H_0: This is the real world game, where the adversary receives commitments under Com_i to msg_0 with tag tag of its choice.

Hybrid H_1: This Hybrid is the same as Hybrid H_0, except the NIZK is replaced with a simulated proof, using the NIZK trapdoor.

Hybrids $H_{2,0}, H_{2,1}, \ldots, H_{2,\tau_{i-1}/2-1}, H_{2,\tau_{i-1}/2}$: In these Hybrid we start switching commitments $c_1, \ldots, c_{\tau_{i-1}/2}$ from commitments to msg_0 to commitments to msg_1. Specifically, in Hybrid $H_{2,j}$, for $j \in \{0, \ldots, \tau_{i-1}/2\}$, commitments c_ℓ, for $\ell \leq j$ are commitments to msg_1 and commitments c_ℓ, for $\ell > j$ are commitments to msg_0. Note that $H_{2,0} \equiv H_1$ and we define $H_2 := H_{2,\tau_{i-1}/2}$.

Hybrid 3: This Hybrid is the same as Hybrid H_2, except the simulated NIZK is switched back to a real NIZK. Note that this Hybrid now corresponds to the real world game, where the adversary receives commitments under Com_i to msg_1.

Claim. With all but negligible probability, $v^{H_0}_{\mathsf{com}} = v^{H_0}_1 = v^{H_0}_2 = \cdots = v^{H_0}_{\tau_{i-1}/2}$.

The claim holds due to the soundness of the i-th level NIZK against adversaries in $\mathcal{DA}_i$.

Claim.

$$(v^{H_0}_{\mathsf{diff}}, \mathsf{out}^{H_0}) \overset{PPT,\mathsf{negl}(n)}{\approx} (v^{H_1}_{\mathsf{diff}}, \mathsf{out}^{H_1})$$

The claim holds due to complexity leveraging. Specifically, the zero knowledge property of the NIZK holds against sub-exponential adversaries, who are strong enough to recover the committed values $v^{H_0}_{\mathsf{diff}}$ and $v^{H_1}_{\mathsf{diff}}$, given the output $c'_1, \ldots, c'_{\tau_{i-1}/2}$.

Claim. For $j \in [\tau_{i-1}/2]$:

$$(v^{H_{2,j-1}}_{\mathsf{diff}}, \mathsf{out}^{H_{2,j-1}}) \overset{\mathcal{DA}_i, O(1/n^{c_{\mathsf{com}}})}{\approx} (v^{H_{2,jl}}_{\mathsf{diff}}, \mathsf{out}^{H_{2,j}})$$

Proof. Assume there is an adversary/distinguisher $(A = (A_1, A_2), D)$ in $\mathcal{DA}_i$ for which the above is not true. We will construct an adversary/distinguisher $(A' = (A'_1, A'_2), D')$ in $\mathcal{DA}_{i-1}$, breaking the non-malleability property of the $(i-1)$-st level commitment.

$A'_1(1^n)$ is specified as follows:

- A'_1 runs $A_1(1^n)$ and obtains output (tag, y) in time $T_i(n) < T_{i-1}(n)$ (where tag is A_1's choice of tag and y is additional output).
- A'_1 runs in uniform time $T'_i(n) \leq T_{i-1}(n)$ to recover the trapdoor td_i for the i-th level (outer) NIZK.
- A'_1 generates $c_1, \ldots, c_{j-1}$ by calling $\mathsf{Com}_{i-1}(\mathsf{msg}_1, \mathsf{tag}_1), \ldots, \mathsf{Com}_{i-1}(\mathsf{msg}_1, \mathsf{tag}_{j-1})$ and generates $c_{j+1}, \ldots, c_{\tau_{i-1}/2}$ by calling $\mathsf{Com}_{i-1}(\mathsf{msg}_0, \mathsf{tag}_{j+1}), \ldots, \mathsf{Com}_{i-}$
- A'_1 outputs tag_j to its challenger, and outputs $(\mathsf{td}_i, y, \mathsf{tag}, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_{\tau_{i-1}/2})$ to A'_2.

On input commitment c_j, generated by a call to Com_{i-1} with tag tag_j, and inputs either $\mathsf{msg}_0, \mathsf{tag}_j$ or $\mathsf{msg}_1, \mathsf{tag}_j$, and values $(\mathsf{td}_i, y, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_{\tau_{i-1}/2})$, generated by A'_1, $A'_2(\mathsf{td}_i, y, \mathsf{tag}, c_1, \ldots, c_{\tau_{i-1}/2})$ is specified as follows:

- A'_2 uses td_i to generate a simulated proof π in fixed polynomial time.
- Run A_2 on input $(y, \mathsf{tag}, c_1, \ldots, c_{\tau_{i-1}/2}, \pi)$.
- Wait for A_2 to output $(c'_1, \ldots, c'_{\tau_{i-1}/2}, \pi', \mathsf{out})$.
- Output $(\perp, \mathsf{out})$ if outputted proof π' does not verify.
- Otherwise, output $(c'_{\ell^*}, \mathsf{out})$, where ℓ^* is the lexicographically first index such that $\mathsf{tag}'_{\ell^*} \notin \mathsf{tag}$. If none exist, then output $(\perp, \mathsf{out})$.

D' is receives as input (v'_j, out) outputted by the above experiment, where v'_j is the committed value v'_j underlying c'_{ℓ^*} (or $\perp$ if the output of A' is $\perp$) and out is the output of A'. Clearly,

$$\Pr_{c_j \leftarrow \mathsf{Com}_{i-1}(\mathsf{msg}_0, \mathsf{tag}_j)}[D'(v'_j, \mathsf{out}) = 1] = \Pr[D(v^{H_{2,j-1}}_{\mathsf{diff}}, \mathsf{out}^{H_{2,j-1}}) = 1]$$

and
$$\Pr_{c_j \leftarrow \mathsf{Com}_{i-1}(\mathsf{msg}_1, \mathsf{tag}_j)}[D'(v'_j, \mathsf{out}) = 1] = \Pr[D(v_{\mathsf{diff}}^{H_{2,j}}, \mathsf{out}^{H_{2,j}}) = 1].$$

Thus, we have that
$$\left| \Pr_{c_j \leftarrow \mathsf{Com}_{i-1}(\mathsf{msg}_0, \mathsf{tag}_j)}[D'(v'_j, \mathsf{out}) = 1] - \Pr_{c_j \leftarrow \mathsf{Com}_{i-1}(\mathsf{msg}_1, \mathsf{tag}_j)}[D'(v'_j, \mathsf{out}) = 1] \right|$$
$$\notin O(1/n^{c_{\mathsf{com}}}).$$
Moreover, A', D' are clearly in $\mathcal{DA}_{i-1}$. Thus, we obtain a contradiction to the $O(1/n^{c_{\mathsf{com}}})$ non-malleability of Com_{i-1} against adversaries in $\mathcal{DA}_{i-1}$.

Claim.
$$(v_{\mathsf{diff}}^{H_2}, \mathsf{out}^{H_2}) \overset{PPT, \mathsf{negl}(n)}{\approx} (v_{\mathsf{diff}}^{H_3}, \mathsf{out}^{H_3}).$$

The claim again holds due to complexity leveraging, as in the proof of indistinguishability for Hybrids H_0 and H_1.

Claim.
$$v_{\mathsf{com}}^{H_3} = v_1^{H_3} = v_2^{H_3} = \cdots = v_{\tau_{i-1}/2}^{H_3}.$$

Again, the claim holds due to the soundness of the i-th level NIZK against $\mathbf{BPtime}(T_{NIZK,i}(n))$ adversaries.

Putting it all together, we get that for any adversary/distinguisher $A, D \in \mathbf{BPtime}(T_i(n)) \bigcap \mathbf{SIZE}(t_i)$, $|\Pr[D(v_{\mathsf{com}}^{H_0}, \mathsf{out}^{H_0}) = 1] - \Pr[D(v_{\mathsf{com}}^{H_3}, \mathsf{out}^{H_3}) = 1]| \in O(1/n^{c_{\mathsf{com}}})$. This completes the proof of Theorem 9.

Acknowledgments

References

AASY16. Benny Applebaum, Sergei Artemenko, Ronen Shaltiel, and Guang Yang. Incompressible functions, relative-error extractors, and the power of nondeterministic reductions. *computational complexity*, 25(2):349–418, Jun 2016.

Bar02. Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. In *43rd FOCS*, pages 345–355. IEEE Computer Society Press, November 2002.

BDKM16. Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin. Non-malleable codes for bounded depth, bounded fan-in circuits. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 881–908. Springer, Heidelberg, May 2016.

BDKM18. Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin. Non-malleable codes from average-case hardness: AC^0, decision trees, and streaming space-bounded tampering. In Nielsen and Rijmen [NR18], pages 618–650.

BDSG+18. Marshall Ball, Dana Dachman-Soled, Siyao Guo, Tal Malkin, and Li-Yang Tan. Non-malleable codes for small-depth circuits. FOCS IEEE Computer Society Press, October 2018. (To appear) Available at https://eprint.iacr.org/2018/207.

BFNW93. Lászzló Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. Bpp has subexponential time simulations unlessexptime has publishable proofs. *computational complexity*, 3(4):307–318, Dec 1993.

BL18. Nir Bitansky and Huijia Lin. One-message zero knowledge and non-malleable commitments. Cryptology ePrint Archive, Report 2018/613, 2018. https://eprint.iacr.org/2018/613.

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

BP04. Boaz Barak and Rafael Pass. On the possibility of one-message weak zero-knowledge. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 121–132. Springer, Heidelberg, February 2004.

CG14. Mahdi Cheraghchi and Venkatesan Guruswami. Capacity of non-malleable codes. In Moni Naor, editor, *ITCS 2014*, pages 155–168. ACM, January 2014.

CGL16. Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In Wichs and Mansour [WM16], pages 285–298.

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, *ICALP 2016*, volume 55 of *LIPIcs*, pages 31:1–31:14. Schloss Dagstuhl, July 2016.

CL17. Eshan Chattopadhyay and Xin Li. Non-malleable codes and extractors for small-depth circuits, and affine functions. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *49th ACM STOC*, pages 1171–1184. ACM Press, June 2017.

CLP13. Kai-Min Chung, Huijia Lin, and Rafael Pass. Constant-round concurrent zero knowledge from P-certificates. In FOCS 2013 [FOC13], pages 50–59.

COSV16. Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Concurrent non-malleable commitments (and more) in 3 rounds. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 270–299. Springer, Heidelberg, August 2016.

COSV17. Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Four-round concurrent non-malleable commitments from one-way functions. In Katz and Shacham [KS17a], pages 127–157.

DDN03. Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM review*, 45(4):727–784, 2003.

DI06. Bella Dubrov and Yuval Ishai. On the randomness complexity of efficient sampling. In Jon M. Kleinberg, editor, *38th ACM STOC*, pages 711–720. ACM Press, May 2006.

DN00. Cynthia Dwork and Moni Naor. Zaps and their applications. In FOCS 2000 [FOC00], pages 283–293.

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

Dru13. Andrew Drucker. Nondeterministic direct product reductions and the success probability of SAT solvers. In FOCS 2013 [FOC13], pages 736–745.

FHMV17. Sebastian Faust, Kristina Hostáková, Pratyay Mukherjee, and Daniele Venturi. Non-malleable codes for space-bounded tampering. In Katz and Shacham [KS17a], pages 95–126.

FL97. Uriel Feige and Carsten Lund. On the hardness of computing the permanent of random matrices. *Computational Complexity*, 6(2):101–132, 1997.

FLS99. Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SIAM Journal on Computing*, 29(1):1–28, 1999.

FMVW14. Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs. Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 111–128. Springer, Heidelberg, May 2014.

FOC00. *41st FOCS*. IEEE Computer Society Press, November 2000.

FOC13. *54th FOCS*. IEEE Computer Society Press, October 2013.

FOC14. *55th FOCS*. IEEE Computer Society Press, October 2014.

FOC17. *58th FOCS*. IEEE Computer Society Press, 2017.

FV11. Lance Fortnow and Salil P. Vadhan, editors. *43rd ACM STOC*. ACM Press, June 2011.

GOS06. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, Heidelberg, August 2006.

Goy11. Vipul Goyal. Constant round non-malleable protocols using one way functions. In Fortnow and Vadhan [FV11], pages 695–704.

GPR16.   Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In Wichs and
            Mansour [WM16], pages 1128–1141.
GRRV14.   Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability.
            In FOCS 2014 [FOC14], pages 41–50.
GSTS03.   Dan Gutfreund, Ronen Shaltiel, and Amnon Ta-Shma. Uniform hardness versus randomness tradeoffs
            for arthur-merlin games. *computational complexity*, 12(3-4):85–130, 2003.
GW02.   Oded Goldreich and Avi Wigderson. Derandomization that is rarely wrong from short advice that is
            typically good. In *International Workshop on Randomization and Approximation Techniques in Computer
            Science*, pages 209–223. Springer, 2002.
HILL99.   Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from
            any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.
HN10.   Danny Harnik and Moni Naor. On the compressibility of $\mathcal{NP}$ instances and cryptographic applications.
            SIAM Journal on Computing, 39(5):1667–1713, 2010.
IW97.   Russell Impagliazzo and Avi Wigderson. P = BPP if E requires exponential circuits: Derandomizing the
            XOR lemma. In *29th ACM STOC*, pages 220–229. ACM Press, May 1997.
Khu17.   Dakshita Khurana. Round optimal concurrent non-malleability from polynomial hardness. In Kalai and
            Reyzin [KR17], pages 139–171.
KR17.   Yael Kalai and Leonid Reyzin, editors. *TCC 2017, Part II*, volume 10678 of *LNCS*. Springer, Heidelberg,
            November 2017.
KS17a.   Jonathan Katz and Hovav Shacham, editors. *CRYPTO 2017, Part II*, volume 10402 of *LNCS*. Springer,
            Heidelberg, August 2017.
KS17b.   Dakshita Khurana and Amit Sahai. How to achieve non-malleability in one or two rounds. In FOCS
            2017 [FOC17], pages 564–575.
KVM02.   Adam R Klivans and Dieter Van Melkebeek. Graph nonisomorphism has subexponential size proofs
            unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002.
Lin03.   Yehuda Lindell. A simpler construction of cca2-secure public-key encryption under general assumptions.
            In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 241–254. Springer, Heidelberg,
            May 2003.
Lip89.   Richard J. Lipton. New directions in testing. In Joan Feigenbaum and Michael Merritt, editors,
            *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey,
            USA, October 4-6, 1989*, pages 191–202, 1989.
LP09.   Huijia Lin and Rafael Pass. Non-malleability amplification. In Michael Mitzenmacher, editor, *41st ACM
            STOC*, pages 189–198. ACM Press, May / June 2009.
LP11.   Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. In
            Fortnow and Vadhan [FV11], pages 705–714.
LPS17.   Huijia Lin, Rafael Pass, and Pratik Soni. Two-round and non-interactive concurrent non-malleable
            commitments from time-lock puzzles. In FOCS 2017 [FOC17], pages 576–587.
LPV08.   Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. Concurrent non-malleable
            commitments from any one-way function. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*,
            pages 571–588. Springer, Heidelberg, March 2008.
Mic00.   Silvio Micali. Computationally sound proofs. *SIAM Journal on Computing*, 30(4):1253–1298, 2000.
MV05.   Peter Bro Miltersen and N Variyam Vinodchandran. Derandomizing arthur–merlin games using hitting
            sets. *Computational Complexity*, 14(3):256–279, 2005.
Nao03.   Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor,
            CRYPTO 2003, volume 2729 of *LNCS*, pages 96–109. Springer, Heidelberg, August 2003.
NR18.   Jesper Buus Nielsen and Vincent Rijmen, editors. *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*.
            Springer, Heidelberg, April / May 2018.
NW94.   Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, October
            1994.
NY90.   Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks.
            In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.
OPVV18.   Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi, and Ivan Visconti. Continuously non-malleable
            codes in the split-state model from minimal assumptions. Cryptology ePrint Archive, Report 2018/542,
            2018. https://eprint.iacr.org/2018/542.
PR05a.   Rafael Pass and Alon Rosen. Concurrent non-malleable commitments. In *46th FOCS*, pages 563–572.
            IEEE Computer Society Press, October 2005.

PR05b.   Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 533–542. ACM Press, May 2005.

PW10.   Rafael Pass and Hoeteck Wee. Constant-round non-malleable commitments from sub-exponential one-way functions. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 638–655. Springer, Heidelberg, May / June 2010.

RSW96.   Ronald L Rivest, Adi Shamir, and David A Wagner. Time-lock puzzles and timed-release crypto. 1996.

Sah99.   Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *40th FOCS*, pages 543–553. IEEE Computer Society Press, October 1999.

STV01.   Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the xor lemma. *Journal of Computer and System Sciences*, 62(2):236 – 266, 2001.

SU05.   Ronen Shaltiel and Christopher Umans. Simple extractors for all min-entropies and a new pseudorandom generator. *Journal of the ACM (JACM)*, 52(2):172–216, 2005.

SU06.   Ronen Shaltiel and Christopher Umans. Pseudorandomness for approximate counting and sampling. *computational complexity*, 15(4):298–341, 2006.

SU09.   Ronen Shaltiel and Christopher Umans. Low-end uniform hardness versus randomness tradeoffs for am. *SIAM Journal on Computing*, 39(3):1006–1037, 2009.

TV00.   Luca Trevisan and Salil P. Vadhan. Extracting randomness from samplable distributions. In FOCS 2000 [FOC00], pages 32–42.

WM16.   Daniel Wichs and Yishay Mansour, editors. *48th ACM STOC*. ACM Press, June 2016.

Yao82.   Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 80–91. IEEE Computer Society, 1982.