An Algebraic Approach to Non-Malleability

Vipul Goyal* Silas Richelson† Alon Rosen‡ Margarita Vald§

Abstract

In their seminal work on non-malleable cryptography, Dolev, Dwork and Naor, showed how to construct a non-malleable commitment with logarithmically-many "rounds"/"slots", the idea being that any adversary may successfully maul in some slots but would fail in at least one. Since then new ideas have been introduced, ultimately resulting in constant-round protocols based on any one-way function. Yet, in spite of this remarkable progress, each of the known constructions of non-malleable commitments leaves something to be desired.

In this paper we propose a new technique that allows us to construct a non-malleable protocol with only a single "slot", and to improve in at least one aspect over each of the previously proposed protocols. Two direct byproducts of our new ideas are a four round non-malleable commitment and a four round non-malleable zero-knowledge argument, the latter matching the round complexity of the best known zero-knowledge argument (without the non-malleability requirement). The protocols are based on the existence of one-way functions and admit very efficient instantiations via standard homomorphic commitments and sigma protocols.

Our analysis relies on algebraic reasoning, and makes use of error correcting codes in order to ensure that committers' tags differ in many coordinates. One way of viewing our construction is as a method for combining many atomic sub-protocols in a way that simultaneously amplifies soundness and non-malleability, thus requiring much weaker guarantees to begin with, and resulting in a protocol which is much trimmer in complexity compared to the existing ones.

Keywords: Non-malleability, commitments, zero-knowle ge

*Microsoft Research, Bangalore. Email: vipul@microsoft.com. Part of this work done while visiting IDC Herzliya.

†UCLA. Email: SiRichel@math.ucla.edu. Work done while visiting IDC Herzliya. Supported by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307952

‡Efi Arazi School of Computer Science, IDC Herzliya, Israel. Email: alon.rosen@idc.ac.il. Work supported by ISF grant no. 1255/12 and by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307952.

§The Blavatnik School of Computer Science, Tel Aviv University, Israel. Email: margarita.vald@cs.tau.ac.il. Work supported in part by ISF grant no. 1255/12.

1 Introduction

The notion of non-malleability is central in cryptographic protocol design. Its objective is to protect against a man-in-the-middle (MIM) attacker that has the power to intercept messages and transform them in order to harm the security in other instantiations of the protocol. Commitment is often used as the paragon example for non-malleable primitives because of its ability to almost "universally" secure higher-level protocols against MIM attacks.

Commitments allow one party, called the committer, to probabilistically map a message m into a string, $\mathrm{Com}(m;r)$, which can be then sent to another party, called the receiver. In the statistically binding variant, the string $\mathrm{Com}(m;r)$ should be *binding*, in that it cannot be later "opened" into a message $m' \neq m$. It should also be *hiding*, meaning that for any pair of messages, m, m', the distributions $\mathrm{Com}(m;r)$ and $\mathrm{Com}(m';r')$ are computationally indistinguishable.

A commitment scheme is said to be *non-malleable* if for every message m, no MIM adversary, intercepting a commitment $\mathrm{Com}(m;r)$ and modifying it at will, is able to efficiently generate a commitment $\mathrm{Com}(\tilde{m};\tilde{r})$ to a related message $\tilde{m}$. Interest in non-malleable commitments is motivated both by the central role that they play in securing protocols under composition (see for example [CLOS02, LPV09]) and by the unfortunate reality that many widely used commitment schemes are actually highly malleable. Indeed, man-in-the-middle (MIM) attacks occur quite naturally when multiple concurrent executions of protocols are allowed, and can be quite devastating.

Beyond protocol composition, non-malleable commitments are known to be applicable in secure multi-party computation [KOS03, Wee10, Goy11], authentication [NSS06], as well as a host of other non-malleable primitives (e.g., coin flipping, zero-knowledge, etc.), and even into applications as diverse as position based cryptography [CGMO09].

1.1 Prior Work

Since their conceptualization by Dolev, Dwork and Naor [DDN91], non-malleable commitments have been studied extensively, and with increasing success in terms of characterizing their round-efficiency and the underlying assumptions required. By now, we know how to construct constant-round non-malleable commitments based on any one-way function, and moreover the constructions are fully black-box. While this might give the impression that non-malleable commitments are well understood, each of the currently known constructions leaves something to be desired.

The first construction, due to DDN is perhaps the simplest and most efficient, mainly because it can in principle be instantiated with highly efficient cryptographic "sub-protocols". This, however, comes at the cost of round-complexity that is logarithmic in the maximum overall number of possible committers. Subsequent works, due to Barak [Bar02], Pass [Pas04], and, Pass and Rosen [PR05] are constant-round, but rely on (highly inefficient) non-black box techniques. Wee [Wee10] (relying on [PW10]) gives a constant-round black-box construction under the assumption that sub-exponentially hard one-way functions exist. This construction employs a generic (and costly) transformation that is designed to handle general "non-synchronizing" MIM adversaries.

Finally, recent works by Goyal [Goy11] and Lin and Pass [LP11] attain non-malleable commitment with constant round-complexity via the minimal assumption that polynomial-time hard to invert one-way functions exist. The Lin-Pass protocol makes highly non-black-box use of the underlying one-way function (though not of the adversary), along with a concept called signature chains;

resulting in significant overhead. Most relevant to the current work is the work of Goyal [Goy11]. Goyal's protocol, using a later result of Goyal, Lee, Ostrovsky and Visconti [GLOV12], can be made fully black-box, with its only shortcomings being high-communication complexity and the use of the Wee transformation (or alternatively a similarly costly transformation due to Goyal [Goy11]) for handling non-synchronizing adversaries. To construct non-malleable commitments, our work follows the blueprint proposed by Goyal, and introduces new proof techniques to significantly trim down its complexity, making various parts of the protocol of Goyal [Goy11] unnecessary.

The current state of affairs is such that in spite of all the remarkable advances, the DDN construction and its analysis remain the simplest and arguably most appealing candidate for non-malleable commitments. This is both due to its black-boxness and because it does not require transformations for handling a non-synchronizing MIM (in fact, the protocol is purposefully designed to introduce asynchronicity in message scheduling, which can be then exploited in the analysis).

1.2 Our Results

In this work we introduce a new algebraic technique for obtaining non-malleability, resulting in a simple and elegant non-malleable commitment scheme. The scheme's analysis contains many fundamentally new ideas allowing us to overcome substantial obstacles without sacrificing efficiency. The protocol is constructed using any statistically binding commitment scheme as a building block, and hence requires the minimal assumption that one way functions exist.

Theorem. *Assume the existence of one-way functions. Then there is a 4−round non-malleable commitment scheme.*

Our protocol enjoys the following appealing features, each of which makes it preferable in at least one way over any of the previously proposed protocols for non malleable commitment:

Simplicity. Compared to all previous protocols, ours is significantly simpler to describe and to instantiate (though not to analyze). The simplicity of the protocol also means that there is no need to introduce costly transformations for handling non-synchronizing adversaries.

Efficiency. In particular, ours is significantly more efficient than all prior protocols both in terms of round complexity, and in the sense that we use a surprisingly small number of sub-protocols, each of which can be instantiated in a very efficient way (e.g. using standard sigma protocols).

Assumption. The assumption underlying our main protocol is the existence of one-way functions, which is necessary for non-malleable commitments.

A direct consequence of our protocol is a 4-round non-malleable zero-knowledge argument based on any OWF. This demonstrates that for zero-knowledge, non-malleability does not necessarily come at the cost of extra rounds of interaction or complexity assumptions.

Theorem. *Assume the existence of one-way functions. Then there is a 4-round black-box non-malleable zero-knowledge argument for every language in NP.*

Beyond the above virtues, we believe that our new techniques are actually the most significant contributions of this work. In addition to our use of algebra, we make novel combinatorial use of error correcting codes in order to ensure that different committers' tags differ in many coordinates (more on that later on). Whereas prior work relied on "worst-case" analysis of differences in committers' tags, ours follows from an "average-case" claim.

One way of viewing our construction is as a method for combining n atomic sub-protocols in a way that simultaneously amplifies their soundness and non-malleability properties, thus requiring much weaker soundness and non-malleability to begin with. We hope that this paradigm will become the norm for future work on in the area as, despite requiring more careful and strenuous analysis, it leads to pleasantly lightweight protocols. For example, this technique alone allows for an immediate linear reduction in communication complexity compared with its nearest relative, Goyal's protocol.

Another payoff of the algebraic techniques we employ is that our protocol only has one "slot". Nearly all of the non-malleable commitment schemes in the literature use multiple slots of interaction as a way to set up imbalances between the two different protocol instantiations that the MIM is involved in. The well known "two slot trick" of [Pas04, PR05, Goy11], for example, is a way to turn an arbitrary asymmetry between the instantiations into two: one which is heavy on the right and one on the left. The inability of the MIM to align the imbalances is crucial to the proof of non-malleability. Running the two slots in parallel introduces several technical problems, most notably "if the two imbalances are side by side, won't they just cancel each other out?" Our analysis uses a computational version of the "linear independence of polynomial evaluation" mantra in order to argue that the MIM cannot combine the two imbalances and must deal with each one separately.

We stress that the use of algebra and error correcting codes does not yield such reward for free: the analysis required becomes substantially more difficult. In the next section we describe and briefly discuss our new protocol and extractor. We then outline our techniques, keeping it informal but pointing out several of the challenges faced and new ideas required to overcome them.

1.3 The New Protocol

Suppose that committer C wishes to commit to message m, and let $t_1, \ldots, t_n \in \mathbb{Z}$ be a sequence of tags that uniquely correspond to C's identity (more on the tags later). Let Com be a statistically binding commitment scheme, and suppose that $m \in \mathbb{F}_q$ where $q > \max_i 2^{t_i}$. The protocol proceeds as follows:

1. C chooses random $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$ and sends $\mathrm{Com}(m)$ and $\{\mathrm{Com}(r_i)\}_{i=1}^n$ to R;
2. R sends C a query vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ where each α_i is drawn randomly from $\left[2^{t_i}\right] \subset \mathbb{F}_q$;
3. C sends R the response $\mathbf{a} = (a_1, \ldots, a_n)$ where $a_i = r_i\alpha_i + m$;
4. C proves in ZK that the values $\mathbf{a}$ (from step 3) are consistent with m and $\mathbf{r}$ (from step 1).

The statistical binding property of the protocol follows directly from the binding of Com. The hiding property follows from the hiding of Com, the zero-knowledge property of the protocol used in step 4, and from the fact that for every i the receiver R observes only a single pair of the form (α_i, a_i), where $a_i = r_i\alpha_i + m$.

Note the role of C's tags in the protocol: t_i determines the size of the $i-$th coordinate's challenge space. Historically, non-malleable commitment schemes have used the tags as a way for the committer to encode its identity into the protocol as a mechanism to prevent M (whose tag is different from C's tag) from mauling. In our protocol the tags play the same role, albeit rather passively. For example, though the size of the $i-$th challenge space depends on t_i, the size of the total challenge space depends only on the sum $\sum_{i=1}^n t_i$ of the tags. In particular, our scheme leaves open the possibility that the left and right challenge spaces might have the same size (in fact this will be ensure by our choice of tags). This raises a re flag, as previous works go to great lengths to set up imbalances between the left an right challenge spaces in or er to force M to "give more information than it gets". Nevertheless, we are able to prove that any mauling attack will fail.

At a very high level, our protocol can be seen as an algebraic abstraction of Goyal's protocol. However, the fun amental ifference we shoul emphasize from [Goy11] is that he crucially relies on the challenge space in the left interaction being much smaller than the challenge space in the right. For us, the challenge spaces in the two interactions are exactly the same size an so the techniques of [Goy11] o not apply to our setting—at least at first. Our protocol oes have small imbalances between the challenge spaces of in ivi ual coor inates, which is what we will eventually use to prove non-malleability. However, proving that the coor inates are sufficiently in epen ent so that these imbalances accrue to something usable is completely new to this work.

1.4 Proving Non-Malleability

Consi er a MIM a versary M that is playing the role of the receiver in a protocol using tags $t_1, \ldots, t_n$ while playing the role of the committer in a protocol using tags $\tilde{t}_1, \ldots, \tilde{t}_n$ (we escribe explicitly how to construct the tags from C's i entity in Section 2). We refer to the former as the "left" interaction an to the latter as the "right" interaction. We let m an $\tilde{m}$ enote the messages committe to in the left an right interactions respectively. One nice feature of our protocol is that it is automatically secure against a non-synchronizing a versary, simply because there are so few roun s, there is no way for the MIM to benefit by changing the message or er: any sche uling but the synchronous one can be ealt with trivially. So the only sche uling our proof actually nee s to han le is a synchronizing one, as epicte in Figure 1 below.

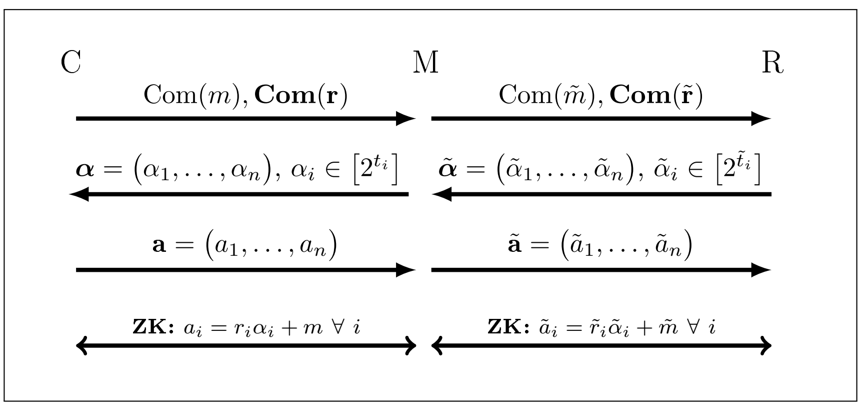

Figure 1: Protocol with Man-in-the-Mi le

Our proof of non-malleability involves emonstrating the existence of an extractor, E, who is able to rewin M an extract $\tilde{m}$ without nee ing to rewin C in the left instantiation. Our extractor is mo ele after Goyal's extractor which: (1) rewin s M to where $\tilde{\boldsymbol{\alpha}}$ was sent an asks a new query $\tilde{\boldsymbol{\beta}}$ instea , an (2) respon s to M's left query ran omly (it cannot o better without rewin ing C as it oes not know m), hoping that M answers correctly on the right.

In Goyal's protocol there is no way for E to know whether M answere correctly or not, an so it must have a verification message after the query response phase so E can compare M's answer with the main threa to verify correctness. We si estep this necessity in the following way. We rewin to the beginning of step 2 twice an ask two new query vectors $\tilde{\boldsymbol{\beta}}$ an $\tilde{\boldsymbol{\gamma}}$, we answer ran omly on the left obtaining $\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\}$, where $(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}})$ is from the main threa . Comparing both $(\tilde{\beta}_i, b_i)$ an $(\tilde{\gamma}_i, c_i)$ with $(\tilde{\alpha}_i, a_i)$ will result in can i ate values $\tilde{m}_i$ an $\tilde{m}_i'$, but with no verification message it is not clear how E shoul verify which one (if either) is correct. We accomplish this with the following "collinearity test". If $\tilde{m}_i = \tilde{m}_i'$ then E checks whether the points $\{(\tilde{\alpha}_i, \tilde{a}_i), (\tilde{\beta}_i, \tilde{b}_i), (\tilde{\gamma}_i, \tilde{c}_i)\}$ are collinear. If so, E eems that $\tilde{m}_i$ was the correct value. This requires proving that M cannot answer "incorrectly but collinearly".

Tags in Error Corrected Form. This iscussion is meant for rea ers who are familiar with the roles of tags in previous non-malleable commitment schemes, for a more thorough intro uction see Section 2. Just as in many of the existing NMC schemes, our protocol consists of n "atomic subprotocols", one for each tag. Previous schemes use the so calle "DDN trick" [DDN91] in or er to turn C's $k-$bit i entity into a list of n $(= k)$ tags $t_1, \dots, t_n$, satisfying the properties: (1) each t_i is of length $\log n + 1$; an (2) if $\{t_i\}_i$ an $\{\tilde{t}_j\}_j$ are the tags resulting from two istinct i entities then there exists some i such that t_i is completely istinct from $\{\tilde{t}_j\}_j$, meaning that $t_i \neq \tilde{t}_j$ for all j.

Previous schemes' security proofs require the extractor to be able to use any completely istinct left subprotocol (i.e., one whose tag is completely istinct from $\{\tilde{t}_j\}_j$) to extract M's commitment $\tilde{m}$ with high probability. This ensures that extraction is possible even in the worst case when there is a single such subprotocol. It also intro uces a goo   eal of re un ancy into the protocol.

While one woul generally expect most pairs of istinct i entities to result in pairs of tags such that property (2) hol s for many i, all the DDN trick can guarantee in the worst case is that it hol s for a single i (since M is allowe to choose his i entity a versarily, this worst case situation might very well be realize). If however, one first applies an error correcting co e to C's i entity obtaining, say, a co ewor in $\mathbb{F}^n$ for suitably chosen finite fiel $\mathbb{F}$ with $|\mathbb{F}| = \mathrm{poly}(n)$, then applying the DDN trick to this co ewor woul yiel tags such that (1) t_i is of length $\mathcal{O}(\log n)$; an (2) t_i is completely istinct from $\{\tilde{t}_j\}_j$ for a constant fraction of the $i \in \{1, \dots, n\}$.

Our "completely istinct on average" property requires only that extraction is possible from a completely istinct left subprotocol with constant probability, since there now are guarantee to be many extraction opportunities. This allows us to remove much of the artificial re un ancy resulting in an incre ibly trim protocol.

Non-malleability against a copying M. To get a sense of why we might expect our scheme to be non-malleable, let us examine the situation against an M who attempts to maul C's commitment by simply copying its messages from the left interaction to the right. Let m be the message committe to on the left an let $\{t_i\}_{i=1}^n$ an $\{\tilde{t}_i\}_{i=1}^n$ be the correspon ing tags.

After the first message, M will have copie C's commitments over to the right interaction, successfully committing to the coefficients of the linear polynomials $\tilde{f}_i(x) = r_i x + m$, $i = 1, \dots, n$. The hi ing of Com ensures it oes not know the polynomials themselves, an so when it receives the right query vector $\tilde{\boldsymbol{\alpha}}$, its only hope of coming up with the correct valuations $\tilde{f}_i(\tilde{\alpha}_i)$ is to copy R's challenge to the left interaction an copy C's response back. However, it is unlikely that this will be possible. In ee , M can only copy $\tilde{\alpha}_i$ over to the left when $\tilde{\alpha}_i \in [2^{t_i}]$. If $\tilde{t}_i > t_i$ then the $i-$th challenge space on the right is at least twice as big as the $i-$th challenge space on the left, which means that the probability $\tilde{\alpha}_i$ can be copie is at most $1/2$. We will use a co e which ensures that

$\tilde{t}_i > t_i$ for a constant fraction of the i, making the probability that M can copy every coor inate of R's query vector $\tilde{\boldsymbol{\alpha}}$ negligible. So M will not be able to successfully answer R's query an complete the proof when performing the "copying" attack.

Non-malleability against general M. Establishing security against a general man-in-the-mi le a versary is significantly more challenging, an this is where the bulk of the new i eas are require . Our proof of non-malleability will require us to elve into the full range of possibilities for M's behavior. In each case, we will show that one of three things happen:

1. M oes not correctly answer its queries with goo enough probability;

2. E succee s in extracting $\tilde{m}$ with sufficient probability;

3. an M with such behavior can be use to break the hi ing of Com.

The core of our result can be seen as a re uction from a PPT M who correctly answers its queries with non-negligible probability an yet causes E to fail, to a machine $\mathcal{A}$ who breaks the hi ing of Com. The following is a very high level outline of our proof.

We efine USEFUL to be the set of transcripts which o not lea to situation 1 above; that is, transcripts for which M has a goo chance of completing the protocol given the prefix. This is important in or er for E to have any chance of successfully extracting $\tilde{m}$. In ee , if M just aborts in every rewin , E will have no chance. From this stan point, USEFUL is the set of transcripts which give E "something to work with." We prove that most transcripts are in USEFUL in Claim 3.

We then efine EXT, the set of "extractable" transcripts, on which E will succee with high probability. These are the transcripts which lea to situation 2. Intuitively, EXT is the set of transcripts such that M has goo probability of correctly answering a query in a rewin espite the fact that E provi es ran om answers to M's queries. We prove that in ee , if a transcript is in EXT then E succee s in extracting $\tilde{m}$.

Finally, we efine TRB, the set of "troublesome" transcripts which are both useful an not extractable. Transcripts in TRB are problematic as on the one han , usefulness ensures that the prefix is such that if M receives correct responses to its queries on the left, it gives correct responses to the queries on the right. At the same time however, transcripts in TRB are not extractable an so the prefix is also such that if M receives ran om responses to its queries on the left it answers the right queries incorrectly. Certainly, the hi ing of Com ensures that M cannot *know* whether it receives correct or ran om responses to its queries on the left. So this ifference in behavior suggests that we may be able to use M to violate the hi ing of Com, lea ing to situation 3 above.

Our main claim in this part of our proof is Claim 8, which says that if the left challenge $\boldsymbol{\alpha}$ has a superpolynomial number of preimage right challenges $\tilde{\boldsymbol{\alpha}}$ then either E succee s in extracting $\tilde{m}$, or M can be use to break hi ing. Such a claim has been at core of the analysis of some previous NMC schemes. In fact, as many previous schemes (such as [Goy11], for example) use multiple slots in or er to *ensure* that some slot has a right challenge space that is much bigger than the left, such a claim often encompasses nearly the entire analysis. In our case, we have some work still left as there is only a single slot an the right an left challenge spaces have the same size. Nevertheless, we are able to prove, using a series of combinatorial arguments, that any mauling attack will win up with M's left query having exponentially many preimage right queries.

To see these techniques in action, efine the set $S = \{i \in [n] : \tilde{t}_i \le t_i\}$, an consi er an M who simply copies the right challenges $\tilde{\alpha}_i$ for $i \in S$ over to the left but who makes sure to pro uce a legal query in the coor inates not in S on the left. As $\left[2^{\tilde{t}_i}\right] \subset \left[2^{t_i}\right]$ for all $i \in S$, copying $\tilde{\alpha}_i$ when $i \in S$ is fine. If we think of M as a map sen ing right challenge $\tilde{\boldsymbol{\alpha}}$ to left challenge $\boldsymbol{\alpha}$, then for any $\tilde{\boldsymbol{\alpha}}_S = (\tilde{\alpha}_i)_{i \in S}$, M sen s $\tilde{\boldsymbol{\alpha}}'$ such that $\tilde{\boldsymbol{\alpha}}'_S = \tilde{\boldsymbol{\alpha}}_S$ to $\boldsymbol{\alpha}'$ such that $\boldsymbol{\alpha}'_S = \tilde{\boldsymbol{\alpha}}_S$. In other wor s, M maps the set of right query vectors whose $S-$coor inates are fixe to $\tilde{\boldsymbol{\alpha}}_S$ to the set of left query vectors whose $S-$coor inates are also fixe to $\tilde{\boldsymbol{\alpha}}_S$. However, the sizes of these subsets of right an left challenges are

$$\prod_{i \notin S} 2^{\tilde{t}_i} \text{ an } \prod_{i \notin S} 2^{t_i},$$

respectively, an $\prod_{i \notin S} 2^{\tilde{t}_i} = 2^{\Omega(n)} \prod_{i \notin S} 2^{t_i}$ (we are using that our tags are in error-correcte form, which ensures $\left|[n] \setminus S\right| = \Omega(n)$). So we see that M, when restricte to the right challenges with $S-$coor inates fixe to $\tilde{\boldsymbol{\alpha}}_S$, is exponentially many to one on average, an so $\boldsymbol{\alpha}$ has exponentially many preimages with high probability.

4−Ro nd Non-Malleability. The protocol in Figure 1 is explaine sequentially, an as written, consists of 8 roun s: two for Naor's commitment, two for the query/response phase, an four for the ZK argument. However, it can be parallelize own to four roun s using the Feige-Shamir four roun ZK argument system [FS90]. This requires running the entire ZK argument in parallel with the commit, query an response messages. We make use of the fact that the statement to be proven can be chosen uring the last roun of the protocol, an that Feige-Shamir is actually an argument of knowle ge, both of which have been use often in the literature. Arme with a 4-roun NMC scheme, 4-roun ZK is obtaine essentially by running a 4-roun ZK argument protocol (we again use Feige-Shamir) in parallel with a non-malleable commitment to the witness w.

Many-Many Non-Malleability. Many-many or concurrent non-malleability consi ers a setting where the MIM can run polynomially many protocols on the left an right (interleave arbitrarily). It can be emonstrate to hol for our protocol using known techniques. First, one can show that our protocol is one-many non-malleable following [Goy11]. The key point is that the extractor we construct uring our proof of non-malleability is able to extract $\tilde{m}$ from the right interaction with high probability, without rewin ing the left execution. Therefore, by the union boun , our extractor will succee in extracting from all of the right interactions with high probability. Next, we use the transformation of [LPV08], that one-many non-malleability implies many-many non-malleability. Their proof uses a hybri argument to say that one-many non-malleability ensures that non-malleability is retaine when a ing polynomially many left executions, one by one.

Using the OWF in a Blackbox Fashion. The protocol escribe in Figure 1 makes non-blackbox use of the OWF uring the ZK part of the protocol. It is often esirable for protocols to make only blackbox use of their buil ing blocks, as the alternative ten s to be vastly less efficient. To this en , the work of [GLOV12] replaces the ZK proof in the [Goy11] NMC scheme with an "MPC in the hea " computation [IKOS07], resulting in a constant roun NMC scheme which makes blackbox use of a OWF. The same transformation works for our protocol as well. We point out, however, that all the ZK argument in our protocol has to o is prove "knowle ge of committe values" an that these values satisfy a linear equation, both of which can be prove very efficiently (*i.e.*, without resorting to costly $\mathcal{NP}-$re uctions), assuming DDH (or other wi ely use har ness assumptions). Therefore, if a statistically bin ing commitment scheme is available that has an efficient proof of knowle ge of committe value, our protocol will be much more efficient than the generic transformation of [GLOV12], which requires C to imagine an entire MPC in his hea .

It is worth noting that irectly plugging in the i eas of [GLOV12] into our protocol results in a 6-roun NMC scheme. We o not a ress the issue of trying to re uce the roun complexity of this blackbox protocol to 4 because our 4-roun non-blackbox protocol is so much faster in practice.

2 Preliminaries

For positive $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$. A function $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is *negligible* if it ten s to 0 faster than any inverse polynomial *i.e.*, for all constants c there exists $n_c \in \mathbb{N}$ such that for every $n > n_c$ it hol s that $\varepsilon(n) < n^{-c}$. We use $\mathbf{negl}(\cdot)$ to specify a generic negligible function. We abbreviate "probabilistic polynomial time" with PPT. We assume familiarity with computational in istinguishability an zero-knowle ge proofs (an relate protocols).

2.1 Commitment schemes

Commitment schemes are protocols which enable a party, known as the committer C, to commit himself to a value while keeping it secret from the (potentially cheating) receiver, R. This property is known as hi ing. A itionally, upon receiving the commitment from C, R is ensure that even if C cheate , there is at most one value that C can ecommit to uring a later, ecommitment phase (bin ing). In this work, we consi er commitment schemes that are statistically-bin ing which means that the hi ing property only hol s against computationally boun e a versaries.

De nition 1 (Statistically Binding Commitment Scheme). *Let* $\langle \mathrm{C}, \mathrm{R} \rangle$ *be an interactive protocol between* C *and* R. *We say that* $\langle \mathrm{C}, \mathrm{R} \rangle$ *is a* statistically bin ing commitment scheme *if the following properties hold:*

Correctness: If C an R o not eviate from the protocol, then R shoul accept (with probability 1) uring the ecommit phase.

Binding: For every C^*, there exists a negligible function $\mathbf{negl}(\cdot)$ such that C^* succee s in the following game with probability at most $\mathbf{negl}(\lambda)$: On security parameter 1^λ: C^* first interacts with R in the commit phase to pro uce commitment c. Then C^* outputs two ecommitments (c, m_0, d_0) an (c, m_1, d_1), an succee s if $m_0 \neq m_1$ an R accepts both ecommitments.

Hiding: For every PPT receiver R^* an every two messages m_0, m_1, the view of R^* after participating in the commitment phase, where C committe to m_0 is in istinguishable from its view after participating in a commitment to m_1.

[Nao91] gives a 2-roun , statistically bin ing bit commitment scheme that can be built from any OWF [HILL99].

2.2 Non-malleable commitments

We wish for our commitment scheme to be impervious to a MIM a versary, M, who takes part in two protocol executions (in the left interaction M acts as the receiver while in the right, M plays the role of the committer), an tries to use the left interaction to affect the right. The security property we esire can be summarize :

For any MIM adversary M*, there exists a standalone machine who plays only one execution as the committer, yet whose commitment is indistinguishable from* M*'s commitment on the right.*

At first glance, non-malleability seems impossible as surely nothing can be one to protect against a MIM who simply copies messages from one protocol execution to another. For this reason, non-malleable security offers protection only against any MIM who tries to change messages in a meaningful way.

On the Existence of Identities. In this work, just as in [DDN91, PR05], we assume that the committer has an i entity $id \in \{0,1\}^k$. In or er to perform a successful mauling attack, a MIM has to maul a commitment correspon ing to C's i entity into a commitment of his own, istinct i entity. Though this soun s like a strong assumption on the network, essentially requiring that "you know who you are talking to", for our purposes, it is actually equivalent to the requirement iscusse above, that the MIM o something other than simply copy messages. This is because our protocol is interactive, an the first committer message contains a statistically bin ing commitment to m. This means that if we set the committer's i entity to be the first committer message, C's an M's i entities will be istinct unless M copie C's first message.

Moving forwar , we assume that the committer's id is externally given an we require that non-malleability hol s only in the case when C an M's i entities are ifferent. We also assume for simplicity that player i entities are known before the protocol begins, though strictly speaking this is not necessary, as the i entities o not appear in the protocol until after the first committer message. We point out that M can choose his i entity a versarially, as long as it is not equal to C's.

De nition of Non-Malleable Commitments. In this work, we consi er the notion of non-malleability with respect to commitment an we will frequently refer to the "message committe to by a MIM a versary M uring the commitment phase". We note that this is uniquely efine , as all commitment schemes in this work are statistically bin ing, an so for all but a negligible fraction of the possible transcripts $\mathbb{T}$ of the interaction between M an an honest receiver R, there exists at most one message m that is consistent with $\mathbb{T}$ (*i.e.*, for which there exist ran om coin tosses which give $\mathbb{T}$). We recall the efinition of non-malleable commitments of Lin et al *et al.* [LPV08].

The man-in-the-middle exec tion. In the man-in-the-mi le execution, the MIM a versary M is simultaneously participating in two interactions calle the left an the right interaction. In the left interaction M is the receiver an interacts with a honest committer whereas in the right interaction M is the committer an interacts with a honest receiver. We efine a ran om variable $\mathbf{MIM}_{\langle \mathrm{C,R} \rangle}(m, z)$ escribing $(\tilde{m}, v)$: the value M commits to in the right interaction, an M's view in the full experiment. Specifically, M has auxiliary information z an interacts on the left with an honest committer C with input message m an i entity id an on the right with honest receiver R. M attempts to commit to a value $\tilde{m}$ that is relate to m using an i entity $\tilde{id}$ of its choice. If the right commitment (as etermine by the transcript) is invali or un efine , or $id = \tilde{id}$ its value is set to $\perp$.

The sim lated exec tion. In the simulate execution a simulator $\mathcal{S}$ interacts with an honest receiver R. $\mathcal{S}$ receives security parameter 1^λ an auxiliary information z an interacts with the honest receiver R. Let $\mathbf{SIM}^{\mathcal{S}}_{\langle \mathrm{C,R} \rangle}(1^\lambda, z)$ enote the ran om variable escribing $(\tilde{m}, v)$: the value $\mathcal{S}$

commits to in the right interaction, an $\mathcal{S}$'s view uring the entire experiment. If the commitment pro uce by $\mathcal{S}$ is invali or un efine , its value is set to $\perp$.

De nition 2 (Non-Malleable Commitments). *A commitment scheme* $\langle \mathrm{C}, \mathrm{R} \rangle$ *is* non-malleable with respect to commitment *if for every PPT MIM adversary* M, *there exists a PPT simulator* $\mathcal{S}$ *such that the following ensembles are indistinguishable:*

$$\{\mathbf{MIM}_{\langle \mathrm{C},\mathrm{R} \rangle}(m, z)\}_{m \in \{0,1\}^\lambda, z \in \{0,1\}^\star}, \text{ and } \{\mathbf{SIM}^{\mathcal{S}}_{\langle \mathrm{C},R \rangle}(1^\lambda, z)\}_{z \in \{0,1\}^\star, id \in \{0,1\}^k}$$

2.3 Tags in Error Corrected Form

In this section, we escribe how to erive the tags from C's i entity, highlighting the properties we will use moving forwar . Let $id \in \{0,1\}^k$ be C's i entity an let $\mathbf{y} \in \mathbb{F}^{n/2}$ be the image of id un er an error correcting co e with constant istance, for a suitable finite fiel $\mathbb{F}$. Constant istance implies that if $id, \tilde{id} \in \{0,1\}^k$ are istinct i entities then $\mathbf{y}$ an $\tilde{\mathbf{y}}$ iffer on a constant fraction of their coor inates. Now, set

$$t_i = \begin{cases} 2i|\mathbb{F}| + y_i, & i \leq n/2 \\ (2n+1)|\mathbb{F}| - t_{n-i+1}, & i > n/2 \end{cases}$$

Note that $2i|\mathbb{F}| \leq t_i < (2i+1)|\mathbb{F}|$ for all i. The following is a list of useful properties that the tags satisfy. Let $\{t_i\}_i$ an $\{\tilde{t}_i\}_i$ be the tags resulting from istinct i entities $id \neq \tilde{id}$.

1. **Ordered:** $t_1 < t_2 < \cdots < t_n$;

2. **Well Spaced:** $t_1 = \omega(\log \lambda)$ an $t_{i+1} - t_i = \omega(\log \lambda)$ for all $i \in [n]$; moreover $t_{i+1} - \tilde{t}_i = \omega(\log \lambda)$.

3. **Good Distance and Balance:** if $i \neq j$ then $t_i \neq \tilde{t}_j$; moreover $t_i < \tilde{t}_i$ hol s for a constant fraction of $i \in [n]$ (as oes $t_i > \tilde{t}_i$).

Properties 1 an 2 follow imme iately as long as $|\mathbb{F}| = \omega(\log \lambda)$. Property 3 follows from 1) the istance of the error correcting co e as $t_i = \tilde{t}_i$ iff $y_i = \tilde{y}_i$ which must not be the case for a constant fraction of the $i \in [n]$; along with 2) if $t_i \neq \tilde{t}_i$ then either $t_i < \tilde{t}_i$ or else $t_{n-i} < \tilde{t}_{n-i}$. This is reminiscent of the two slot trick of [Pas04, PR05].

It remains to select parameters. Note that we have alrea y touche on the role that the tags play in our protocol: the size of the challenge space in coor inate i is 2^{t_i}. This means that we woul like to make the tags as small as possible, while still allowing our security proof to go through. We make the conservative selection $n = \mathcal{O}(\lambda)$ an $|\mathbb{F}| = \log^2(\lambda)$ to ensure both that the above properties hol an that all that is require of the error correcting co e is that it has constant istance an constant rate. Co es with such properties are known to exist. We coul use, for example polynomial base co es such as Ree -Muller co es, the multivariate generalization of Ree -Solomon co es. This results in the overall communication complexity of our non-malleable commitment scheme being $\tilde{\mathcal{O}}(\lambda^2)$. Slightly better communication complexity might be available through more agressive choices of parameters or better co es. We o not press the issue further.

3 The Protocol

In this section, we escribe our protocol given tags $t_1, \ldots, t_n$ in error correcte form as escribe in Section 2.3. We use Naor's two roun , statistically bin ing bit commitment scheme [Nao91] as a buil ing block.[1] We use bol face to enote vectors; in particular a challenge vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ an a response vector $\mathbf{a} = (a_1, \ldots, a_n)$. We write **Com** for the entire first commitment message, so $\mathbf{Com} = \big(\mathrm{Com}(m), \mathrm{Com}(r_1), \ldots, \mathrm{Com}(r_n)\big)$. Our non-malleable commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle$ between a committer C trying to commit to m an a receiver R appears in Figure 2. The ecommitment phase is one by having the committer C sen m an the ran omness it use uring the protocol.

P blic Parameters: Tags $t_1, \ldots, t_n$ an a large prime q such that $q > 2^{t_i}$ for all i.

Commiter's Pri ate Inp t: Message $m \in \mathbb{F}_q$ to be committe to.

Commit Phase:

0. R $\to$ C **Initialization message:** Sen the first message σ of the Naor commitment scheme.
1. C $\to$ R **Commit message:** Sample ran om $r_1, \ldots, r_n \in \mathbb{F}_q$ an $s, s_1, \ldots, s_n$.
   - Define linear functions $f_1, \ldots, f_n$ by $f_i(x) = r_i x + m$.
   - Sen commitments $\mathbf{Com} = \big(\mathrm{Com}_\sigma(m; s), \mathrm{Com}_\sigma(r_1; s_1), \ldots, \mathrm{Com}_\sigma(r_n; s_n)\big)$.
2. R $\to$ C **Q ery:**
   - Sen ran om challenge vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in [2^{t_i}] \subset \mathbb{F}_q$.
3. C $\to$ R **Response:**
   - Sen evaluation vector $\mathbf{a} = (a_1, \ldots, a_n)$, $a_i = f_i(\alpha_i)$.
4. C $\longleftrightarrow$ R **Consistency proof:** Parties engage in a zero-knowle ge argument protocol where C proves to R that $\exists \big((m, s), (r_1, s_1), \ldots, (r_n, s_n)\big)$ such that:
   - $\mathbf{Com} = \big(\mathrm{Com}_\sigma(m; s), \mathrm{Com}_\sigma(r_1; s_1), \ldots, \mathrm{Com}_\sigma(r_n; s_n)\big)$; an
   - $a_i = r_i \alpha_i + m \ \forall\ i = 1, \ldots, n$.

Decommit Phase:

C $\to$ R **Decommit Message:** Sen $\big((m, s), (r_1, s_1), \ldots, (r_n, s_n)\big)$.

Veri cation: R checks the correctness of the commit an response messages.

Figure 2: The non-malleable commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle$.

Proposition 1. *The commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle$ is computationally hiding and statistically binding.*

[1] Briefly recall Naor's scheme: 1) R sends random initialization message σ, and 2) C responds with $\mathrm{Com}_\sigma(m; s)$, a commitment to $m \in \{0, 1\}$ using randomness s (we will feel free to just write $\mathrm{Com}(m)$, surpressing σ and s for simplicity). We comment that the same initialization message σ can be used for polynomially many parallel instantiations of the scheme, allowing C to commit to $m \in \mathbb{Z}_q$ one bit at a time (actually [Nao91] shows how to commit to longer messages more efficiently).

Proof Sketch. Statistical bin ing follows from the statistical bin ing property of the un erlying commitment scheme Com. To prove computational hi ing, we consi er the following hybri experiments.

1. Simulate the ZK consistency proof step. In istinguishability follows from the ZK property.

2. For each $i \in [n]$, replace the commitment $\mathrm{Com}(r_i)$ to be a commitment to ran om value. In istinguishability follows from the hi ing of Com.

3. Replace the polynomials with ran om polynomials $\bar{f}_1, \ldots, \bar{f}_n$ such that $\bar{f}_i(\alpha_i) = f_i(\alpha_i)$ an $\bar{f}_i(0) = m'$ for ran omly sample m' an all $i \in [n]$. The in istinguishability follows from having $n+1$ variables an only n equations.

4. Change the commitment $\mathrm{Com}(m)$ to be a commitment to a ran om string (as oppose to a commitment to m). In istinguishability follows from the hi ing of Com.

In the final hybri , the transcript of the commitment stage contains no information about the value m being committe to, an so no information about m is leake by the protocol. □

Theorem 1 (Main theorem). *The commitment scheme* $\langle \mathrm{C}, \mathrm{R} \rangle$ *is non-malleable against a synchronizing adversary.*

We comment that non-malleability against a general *non-synchronizing* a versary actually hol s in the above protocol (provi e we choose a ZK with suitable properties, such as [FS90]). However, we only prove non-malleability against a synchronizing MIM (*i.e.*, one who plays correspon ing messages of the two instantiations one after the other) because the large number of messages of the protocol above make it cumbersome to examine all possibilities for M's sche uling.

We efer the proof of non-malleability against non-synchronizing M until after we parallelize our protocol own to four roun s (see Section 6). This makes it much easier (in fact trivial) to irectly examine all of the non-synchronizing options for message sche uling that M has available.

4 Proof of Non-Malleability

In this section we prove Theorem 1. Recall from Definition 2 that we must show that for any PPT MIM M there exists a PPT simulator $\mathcal{S}$ such that

$$\left\{\mathbf{MIM}_{\langle \mathrm{C},\mathrm{R}\rangle}(m,z)\right\}_{m,z} \approx_c \left\{\mathbf{SIM}^{\mathcal{S}}_{\langle \mathrm{C},\mathrm{R}\rangle}(1^\lambda,z)\right\}_{z,id},$$

where the istributions output $(\tilde{m}, v)$: the commitment in the right interaction an view after the commit phases of both executions are complete in the real an i eal worl s, respectively. Our simulator is a very simple machine who runs M internally, committing honestly to $0 \in \mathbb{Z}_q$ on the left an forwar ing M's messages on the right to an honest receiver R.

We prove in istinguishability of the above istributions for any M by constructing an extractor E which takes M's view after the commit phases of the left an right executions are complete an outputs its commitment $\tilde{m}$ in the right execution whp. It follows that an algorithm which istinguishes $\mathcal{D}_0 = \left\{\mathbf{MIM}_{\langle \mathrm{C},\mathrm{R}\rangle}(m,z)\right\}_{m,z}$ from $\mathcal{D}_1 = \left\{\mathbf{SIM}^{\mathcal{S}}_{\langle \mathrm{C},\mathrm{R}\rangle}(1^\lambda,z)\right\}_{z,id}$ can be use to break the hi ing of $\langle \mathrm{C}, \mathrm{R} \rangle$ in the following way: 1) let v be M's view after completing the commit phases of the left an right executions in either the real or i eal worl ; 2) use E to obtain the pair $(\tilde{m}, v)$;

3) use the istinguisher to etermine whether M's interaction took place in the real or i eal worl . This breaks the hi ing of the left commitment as the only ifference between the worl s is that in the real, C commits to m while in the i eal, $\mathcal{S}$ commits to 0.

Formally, we assume that there exists a PPT istinguisher D such that

$$\left|\Pr_{(\tilde{m},v)\leftarrow\mathcal{D}_0}\big(\mathrm{D}(\tilde{m},v)=1\big)-\Pr_{(\tilde{m},v)\leftarrow\mathcal{D}_1}\big(\mathrm{D}(\tilde{m},v)=1\big)\right|\geq 2p$$

for some non-negligible $p=p(\lambda)$. We prove that E succee s with probability at least $1-p$. Note this suffices for proving non-malleability since it means that E extracts $\tilde{m}$ AND the D will use $(\tilde{m},v)$ to etermine whether M is interacting with C committing to m, or $\mathcal{S}$ committing to 0. We also assume without loss of generality that M is eterministic an that M's probability of successfully completing the protocol (over C's an R's ran om coins) is at least p.

4.1 The Extractor E

The high level escription of our extractor (escribe formally in Figure 3) is quite simple. Intuitively, our protocol begins by C committing to n, threshol 2, Shamir secret sharings [Sha79] of m; R then asks for one ran om share from each sharing, which C gives. All E oes is rewin M to the beginning of the right session's query phase ask for a new ran om share. Since E gets one share as part of its input, this will allow E to reconstruct $\tilde{m}$.

The problem with this approach is that E oes not know the value C has committe to on the left an so it oes not know how to answer M's query on the left correctly. The best E can o is give a ran om response on the left an hope that M will give a correct response on the right anyway. On the one han , the hi ing of Com ictates that M cannot istinguish a correct response from a ran om one. On the other han , M oesn't actually nee to know whether the response on the left is correct or not in or er to perform a successful mauling attack. Imagine, for example, the MIM who mauls R's challenge to the left execution an mauls C's response back. Such an M will prevent E from extracting $\tilde{m}$ because M only correctly answers E's query if given a correct response to its own left query, which E cannot give. Of course we will prove that no M with such behavior can exist, but this proof is highly non-trivial.

Another question which our extractor raises is "how can E tell a correct response from an incorrect one?" As we have escribe it, the hi ing of Com ensures that it cannot. However, a small mo ification to the E escribe above fixes this. Instea of asking for one new share, E rewin s twice to the beginning of the right query phase an asks for two ifferent new shares.

The key observation is that if M answers both queries correctly then the three shares it hol s (the two it receive plus the one it got as input) are collinear, whereas if M answers at least one incorrectly they are overwhelmingly likely to NOT be collinear. This is the first appearance of a tangeable payoff of the algebraicity of our protocol. For example, the protocol of [Goy11] (which is similar to ours, but strictly combinatorial in nature) oes not have this algebraic verification technique at its isposal an must intro uce use extra roun s into the protocol to ensure its extractor can reconstruct $\tilde{m}$.

E is given as input a transcript of a complete commit phase in both the left an right interactions. We enote the transcript with the letter $\mathbb{T}$. Specifically,

$$\mathbb{T}=\big(\mathbf{Com},\tilde{\mathbf{Com}},\boldsymbol{\alpha},\tilde{\boldsymbol{\alpha}},\mathbf{a},\tilde{\mathbf{a}},\pi,\tilde{\pi}\big).$$

Since E will not be intereste in the proofs $(\pi, \tilde{\pi})$, an since M is eterministic (an so $\tilde{\mathbf{Com}}$, $\boldsymbol{\alpha}$, $\tilde{\mathbf{a}}$ are uniquely etermine by $\mathbf{Com}, \tilde{\boldsymbol{\alpha}}$, an $\mathbf{a}$) we will often just write $\mathbb{T} = \big(\mathbf{Com}, \tilde{\boldsymbol{\alpha}}, \mathbf{a}\big)$.

De nition 3 (**Accepting Transcript**). *We say that* $\mathbb{T} \in \mathsf{ACC}$ *if both* π *and* $\tilde{\pi}$ *are accepting proofs.*

The soun ness of the ZK ensures that if $\mathbb{T} \in \mathsf{ACC}$ then query vectors $\tilde{\boldsymbol{\alpha}}$ an $\boldsymbol{\alpha}$ are answere correctly. We say that M aborts if M behaves in such a way as to make $\mathbb{T} \notin \mathsf{ACC}$. Note this inclu es the case when M acts in an obviously corrupt fashion, causing C or R to abort.

The extractor E gets $\mathbb{T} \in \mathsf{ACC}$ as input so the probabilities which arise in our analysis often are con itione on the event $\mathbb{T} \in \mathsf{ACC}$. We enote this with the convenient shorthan $\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\cdots\big)$ instea of $\Pr_{\mathbb{T}}\big(\cdots \big| \mathbb{T} \in \mathsf{ACC}\big)$. For fixe **Com**, M can be thought of as a eterministic map, mapping right query vectors to left ones. We write $\boldsymbol{\alpha} = \mathrm{M}(\tilde{\boldsymbol{\alpha}})$ to be consistent with this point of view. We assume that the transcript E gets as input is consistent with exactly one right commitment $\tilde{m}$. As $\langle \mathrm{C}, \mathrm{R}\rangle$ is statistically bin ing, this happens with overwhelming probability.

See Figure 3 below for a formal escription of the extractor. Note that there are two ways for E to fail to output $\tilde{m}$. The first is if E fails to extract any value an outputs **FAIL**. The other is if E acci entally extracts an incorrect value $\tilde{m}' \neq \tilde{m}$.

Tags: Let $\{t_i\}_i$ an $\{\tilde{t}_i\}_i$ be the left an right tags, respectively, in error correcte form.

Inp t: $\mathbb{T} = \big(\mathbf{Com}, \tilde{\boldsymbol{\alpha}}, \mathbf{a}\big) \in \mathsf{ACC}$, an a large value $N = \mathrm{poly}(\lambda)$. E is given oracle access to M.

Extraction proced re: For $j \in [N]$:

1. Rewin M to the beginning of step 2 of the protocol:
   - generate a ran om right challenge vector $\tilde{\boldsymbol{\beta}}_j = (\tilde{\beta}_{1,j}, \ldots, \tilde{\beta}_{n,j})$, where $\tilde{\beta}_{i,j} \in [2^{\tilde{t}_i}]$.
   - Fee M with $\tilde{\boldsymbol{\beta}}_j$ an receive challenge $\boldsymbol{\beta}_j = (\beta_{1,j}, \ldots, \beta_{n,j})$ for left interaction.
2. Fee $\mathbf{b}_j = (b_{1,j}, \ldots, b_{n,j})$ to M where $b_{i,j} = \begin{cases} a_i, & \beta_{i,j} = \alpha_i \\ r \xleftarrow{\mathrm{R}} \mathbb{Z}_q, & \beta_{i,j} \neq \alpha_i \end{cases}$. Get $\tilde{\mathbf{b}}_j = (\tilde{b}_{1,j}, \ldots, \tilde{b}_{n,j})$.
3. For each $i \in [n]$ use $\big\{(\tilde{\alpha}_i, \tilde{a}_i), (\tilde{\beta}_{i,j}, \tilde{b}_{i,j})\big\}$ to interpolate a line an recover can i ate $\tilde{m}_{i,j}$.
4. Repeat steps 1-3. Let $\tilde{\boldsymbol{\gamma}}_j = (\tilde{\gamma}_{1,j}, \ldots, \tilde{\gamma}_{n,j})$ be new right challenge vector an $\tilde{\mathbf{c}}_j = (\tilde{c}_{1,j}, \ldots, \tilde{c}_{n,j})$ be correspon ing response. Let $(\tilde{m}'_{1,j}, \ldots, \tilde{m}'_{n,j})$ be recovere can i ates.
5. If for some $i \in [n]$, $\tilde{m}_{i,j} = \tilde{m}'_{i,j}$ an $\big\{(\tilde{\alpha}_i, \tilde{a}_i), (\tilde{\beta}_{i,j}, \tilde{b}_{i,j}), (\tilde{\gamma}_{i,j}, \tilde{c}_{i,j})\big\}$ are collinear output $\tilde{m}_{i,j}$ an halt.

O tp t: Output **FAIL**.

Figure 3: The Extractor E.

Theorem 2 (**S cient for Theorem 1**). *Let* E *be the extractor described in Figure 3, and let* $\mathbb{T}$ *be the transcript it is given as input. Let* $\tilde{m}$ *be* M*'s commitment in the right interaction of* $\mathbb{T}$*. Then*

$$\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathrm{E}(\mathbb{T}) \neq \tilde{m}\big) \leq p,$$

where the probability is over $\mathbb{T} \in \mathsf{ACC}$ *and the randomness of* E.

4.2 Extractable, Useful and Troublesome Transcripts

We now begin to chip away at Theorem 2 by examining special classes of transcripts on which a mauling attack will fail. This allows us to gather properties which the remaining pertinent transcripts must satisfy which will ai our future analysis. In this section we focus on the commitment message of the protocol.

Recall the two ways E can fail: by outputting **FAIL** or by outputting incorrect $\tilde{m}' \neq \tilde{m}$. Note that the secon way requires M to answer a pair of queries incorrectly but in such a way so that they yiel the same can i ate message an they pass the collinearity test. In this case we say that M answers *incorrectly but collinearly.*

De nition 4 (**Incorrect b t Collinear**). *Fix a main thread transcript* $\mathbb{T} = (\mathbf{Com}, \tilde{\boldsymbol{\alpha}}, \boldsymbol{a})$ *and an* $i \in \{1, \ldots, n\}$*. Let* $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{b}})$ *and* $(\tilde{\boldsymbol{\gamma}}, \tilde{\boldsymbol{c}})$ *denote two query/response pairs arising during the execution of* E *while rewinding* M*. Suppose that interpolating* $(\tilde{\beta}_i, \tilde{b}_i)$ *and* $(\tilde{\gamma}_i, \tilde{c}_i)$ *against the main thread's point* $(\tilde{\alpha}_i, \tilde{a}_i)$ *produces the same candidate message* $\tilde{m}'$*. We say that* M *answers* $(\tilde{\beta}_i, \tilde{\gamma}_i)$ incorrectly but collinearly *if:*

. $\tilde{m}' \neq \tilde{m}$*; and*

. $\big\{(\tilde{\alpha}_i, \tilde{a}_i), (\tilde{\beta}_i, \tilde{b}_i), (\tilde{\gamma}_i, \tilde{c}_i)\big\}$ *are collinear.*

We define the set $\mathsf{IBC}^i(\mathbf{Com}, \tilde{\alpha}_i) = \big\{(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) : \mathrm{M} \text{ answers } (\tilde{\beta}_i, \tilde{\gamma}_i) \text{ incorrectly but collinearly}\big\}$*. Finally, define*

$$\mathsf{IBC}(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) = \big\{\mathbb{T} \in \mathsf{ACC} : (\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) \in \mathsf{IBC}^i(\mathbf{Com}, \tilde{\alpha}_i) \textit{ for some } i\big\}.$$

Note that $\mathsf{IBC}^i(\mathbf{Com}, \tilde{\alpha}_i)$ is well efine given $\mathbb{T}$ an E's ran omness. Intuitively IBC is the set of transcripts for which E might fail because M answers incorrectly but collinearly. The following claim shows that these transcripts rarely occur.

Claim 1. *For any* $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}})$*,* $\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{IBC}(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}})\big) = \mathbf{negl}(\lambda)$.

Proof. Fix $i \in \{1, \ldots, n\}$ an let $\mathbb{T}, \mathbb{T}' \in \mathsf{ACC}$ be main threa s with the same prefix $\mathbf{Com}$ but iffer- ent i−th right queries $\tilde{\alpha}_i$ an $\tilde{\alpha}'_i$. Moreover, fix E's ran omness arbitrarily making it eterministic, so that the sets $\mathsf{IBC}^i(\tilde{\alpha}_i)$ an $\mathsf{IBC}^i(\tilde{\alpha}'_i)$ are efine . Note that $\mathsf{IBC}^i(\tilde{\alpha}_i)$ an $\mathsf{IBC}^i(\tilde{\alpha}'_i)$ are isjoint. In ee , suppose $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) \in \mathsf{IBC}^i(\tilde{\alpha}_i) \cap \mathsf{IBC}^i(\tilde{\alpha}'_i)$. Then the four points

$$\big\{(\tilde{\alpha}_i, \tilde{a}_i), (\tilde{\alpha}'_i, \tilde{a}'_i), (\tilde{\beta}_i, \tilde{b}_i), (\tilde{\gamma}_i, \tilde{c}_i)\big\}$$

are collinear. This means that the line they all lie on is correct because $(\tilde{\alpha}_i, \tilde{a}_i)$ an $(\tilde{\alpha}'_i, \tilde{a}'_i)$ are correct ($\mathbb{T}, \mathbb{T}' \in \mathsf{ACC}$) an so $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) \notin \mathsf{IBC}^i(\tilde{\alpha}_i) \cup \mathsf{IBC}^i(\tilde{\alpha}'_i)$ as M answere $\tilde{\beta}_i$ an $\tilde{\gamma}_i$ correctly. Therefore, for a fixe prefix $\mathbf{Com}$ an extractor queries $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}})$, there is at most one value of $\tilde{\alpha}_i$ such that $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) \in \mathsf{IBC}^i(\tilde{\alpha}_i)$. As the set of possible $\tilde{\alpha}_i$ is superpolynomial, the chances that R's query $\tilde{\boldsymbol{\alpha}}$ in $\mathbb{T}$ is such that $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}) \in \bigcup_i \mathsf{IBC}^i(\tilde{\alpha}_i)$ for any extractor query $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}})$ is negligible. The result follows. $\square$

As our extractor only asks polynomially many pairs of new queries $(\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}})$, we see that E outputs the wrong message $\tilde{m}' \neq \tilde{m}$ with negligible probability. This means that if E fails, it oes so because it oes not receive correct answers to its queries. We efine EXT, the set of "extractable" transcripts, on which M has a non-negligible chance of answering a query correctly even given that its queries are answere by E.

De nition 5 (**Extractable Transcripts**). *Fix $\varepsilon^* = \big(\lambda/N\big)^{1/2}$. We define*

$$\mathsf{EXT}_i = \big\{(\mathbf{Com}, \tilde{\boldsymbol{\alpha}}) : \Pr_{\tilde{\boldsymbol{\beta}}}\big(\mathrm{M} \textit{ correctly answers } \tilde{\beta}_i \big| \mathbf{Com} \ \&\ \mathrm{M}\textit{'s queries answered by } \mathrm{E}\big) \geq \varepsilon^*\big\}.$$

Set $\mathsf{EXT} = \big\{\mathbb{T} \in \mathsf{ACC} : (\mathbf{Com}, \tilde{\boldsymbol{\alpha}}) \in \mathsf{EXT}_i$ *for some* $i\big\}$.

Intuitively, EXT is the set of transcripts such that M has goo probability of provi ing at least one pair of correct answers to a pair of queries aske in a rewin espite the fact that E provi es ran om answers to M's queries. We now prove that if a transcript is in EXT then E succee s in extracting $\tilde{m}$ whp.

Claim 2. $\Pr_{\mathbb{T}}\big(\mathrm{E}(\mathbb{T}) = \mathbf{FAIL} \big| \mathbb{T} \in \mathsf{EXT}\big) = \mathbf{negl}(\lambda)$, *where the probability is over $\mathbb{T}$ and the randomness of* E.

Proof. Let $\mathbf{E}_j$ be the event that there exists an i such that M answers both $i-$th queries correctly in rewin j. Since $\mathbb{T} \in \mathsf{EXT}$ we have that $\Pr(\mathbf{E}_j) \geq (\varepsilon^*)^2 = \lambda/N$ for all j. As the $\mathbf{E}_j$ are in epen ent,

$$\Pr_{\mathbb{T}}\big(\mathrm{E}(\mathbb{T}) = \mathbf{FAIL} \big| \mathbb{T} \in \mathsf{EXT}\big) = \Pr(\text{not } \mathbf{E}_j\ \forall\ j \big| \mathbb{T} \in \mathsf{EXT}) \leq \left(1 - \frac{\lambda}{N}\right)^N = \mathbf{negl}(\lambda).$$

□

Having looke at transcripts on which E succee s whp, we next examine a set of transcripts on which E trivially fails. These are transcripts which M was lucky to complete given the commitment phase. In ee , if every time E rewin s M simply aborts, E will have no chance of extracting $\tilde{m}$.

De nition 6 (**Usef l Transcripts**). *Fix non-negligible $\delta < \frac{1}{3}$ and (temporarily) define*

$$W = \big\{\mathbf{Com} : \Pr_{\mathbb{T}}\big(\mathbb{T} \in \mathsf{ACC} \big| \mathbf{Com}\big) \leq \delta p^2\big\}.$$

Set $\mathsf{USEFUL} := \big\{\mathbb{T} \in \mathsf{ACC} : \mathbf{Com} \notin W\big\}$.

Informally, W is the set of partial transcripts for which M is unlikely to complete the protocol, so USEFUL is the set of transcripts such that if M is rewoun an execute again on a ifferent query, the protocol will complete successfully with goo probability. We note that most transcripts are in ee useful.

Claim 3. $\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \notin \mathsf{USEFUL}\big) \leq \delta p$.

Proof. We have

$$\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbf{Com} \in W\big) = \Pr_{\mathbb{T}}\big(\mathbf{Com} \in W \big| \mathbb{T} \in \mathsf{ACC}\big) \leq \frac{\Pr_{\mathbb{T}}\big(\mathbb{T} \in \mathsf{ACC} \big| \mathbf{Com} \in W\big)}{\Pr_{\mathbb{T}}(\mathbb{T} \in \mathsf{ACC})} \leq \delta p,$$

using the efinition of W an the fact that $\Pr_{\mathbb{T}}(\mathbb{T} \in \mathsf{ACC}) \geq p$. □

Transcripts in EXT are those for which M is likely to correctly answer a right query even given incorrect responses to its own left queries. On the other han , USEFUL can be thought of as the transcripts for which M answers the right queries correctly if given correct answers to its left queries. This lea s us to the following efinition.

De nition 7 (Tro blesome Transcripts). *We define* $\mathsf{TRB} = \mathsf{USEFUL} \setminus \mathsf{EXT}$.

Transcripts in TRB are troublesome as essentially, they are transcripts for which M answers the right queries correctly if given correct answers to its left queries, but incorrectly if given incorrect answers to its left queries. Certainly, the hi ing of Com ensures that M cannot *know* whether it receives correct or ran om responses to its queries on the left. So this ifference in behavior suggests that we may be able to use M to break the hi ing of Com. However, it is not so easy. Keep in min , M oes not have to know whether it is giving a correct or incorrect answer on the left. In ee , almost all mauling attacks one coul imagine have the property that M answers correctly on the right if an only if it gets correct answers on the left. The following lemma comprises the heart of our analysis.

Lemma 1. *If* Com *is computationally hiding then there exists a constant* $\delta' < \frac{1}{3}$ *such that*

$$\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\big) \le \delta' p.$$

Lemma 1 combine with Claims 1 through 3 give us

$$\begin{aligned} \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathrm{E}(\mathbb{T})\neq\tilde{m}\big) &\le \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\notin\mathsf{USEFUL}\big)+\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\big)\\ &+ \Pr_{\mathbb{T}}\big(\mathrm{E}(\mathbb{T})=\mathbf{FAIL}\big|\mathbb{T}\in\mathsf{EXT}\big)\\ &+ \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{IBC}(\tilde{\boldsymbol{\beta}},\tilde{\boldsymbol{\gamma}})\text{ for some }(\tilde{\boldsymbol{\beta}},\tilde{\boldsymbol{\gamma}})\text{ aske by E}\big)\\ &\le \delta p+\delta' p+\mathbf{negl}(\lambda)<p, \end{aligned}$$

proving Theorem 2.

5 Proof of Lemma 1

5.1 Proof Overview

We prove Lemma 1 by efining the notion of "query epen ence", an then consi ering the possible ifferent ways in which M's left queries $\boldsymbol{\alpha}$ can epen on right queries $\tilde{\boldsymbol{\alpha}}$. Intuitively, $\alpha_{i'}$ being epen ent on $\tilde{\alpha}_i$ is the result of M performing a mauling attack. Suppose that M mauls $\mathrm{Com}(f_{i'})$ in or er to obtain $\mathrm{Com}(\tilde{f}_i)$. Then M oes not know $\tilde{f}_i$ an so cannot hope to answer $\tilde{\alpha}_i$ except by mauling C's answer to $\alpha_{i'}$. Therefore, if M is rewoun to the beginning of step 2 an aske a ifferent query vector $\tilde{\boldsymbol{\beta}}$ such that $\tilde{\beta}_i = \tilde{\alpha}_i$, M will have to ask $\boldsymbol{\beta}$ such that $\beta_{i'} = \alpha_{i'}$ if it wants to answer successfully. This is the i ea of query epen ence: if $\tilde{\alpha}_i$ is aske on the right, then $\alpha_{i'}$ must be aske on the left.

Recall that in the intro uction we consi ere a copying MIM who attempts to maul C's commitment by simply copying an pasting messages between the left an right sessions. Such an attack is a very simple example of a mauling attack in which each α_i is epen ent on $\tilde{\alpha}_i$. We saw this attack is foile by the large number of left tags which iffer from all right tags, preventing the right query $\tilde{\boldsymbol{\alpha}}$ from being a legal left query except with negligible probability. In fact, we prove in Claim 7 that all mauling attacks in which each α_i epen s on $\tilde{\alpha}_i$ will fail whp.

This encourages us to investigate what else can happen. We arrive at three possibilities.

- **UNBAL:** There exist $i' > i$ such that $\alpha_{i'}$ epen s on $\tilde{\alpha}_i$.
- **1−2:** There exist (i_1, i_2, i') such that $\alpha_{i'}$ epen s on both $\tilde{\alpha}_{i_1}$ an $\tilde{\alpha}_{i_2}$.
- **IND:** There exists i such that each $\alpha_{i'}$ oes *not* epen on $\tilde{\alpha}_i$.

In the actual proof we formalize the above possibilities using precise con itional probability statements. We keep it informal here, however, in or er to convey as much intuition as possible.

Note that if none of the above three events occur then α_i epen s on $\tilde{\alpha}_i$ for all i which is what we hope happens. We complete the proof by showing that each of the three events cannot happen except with very small probability. However, this is easier sai than one. Consi er, for example, the mauling attack which results in 1−2. Intuitively, if $\alpha_{i'}$ is epen ent on both $\tilde{\alpha}_{i_1}$ an $\tilde{\alpha}_{i_2}$ then M is using C's response $f_{i'}(\alpha_{i'})$ on the left to pro uce both $\tilde{f}_{i_1}(\tilde{\alpha}_{i_1})$ an $\tilde{f}_{i_2}(\tilde{\alpha}_{i_2})$ on the right. On the one han it is extremely unlikely that a single polynomial evaluation on the left contains enough information to allow M to correctly give two ran om evaluations on the right. On the other han , this intuition alone isn't enough to say that 1−2 can't occur as the argument is information theoretic in nature. In ee , any statment one wishes to make about M's behavior in the query phase must have a computational proof as an unboun e M can query however it wants to an then simply break the hi ing of the commitments in the first message to learn the $\tilde{f}_i$ an answer correctly.

The key claim which allows us to capitalize on our information theoretic intuition is Claim 8 which states that if the left query $\boldsymbol{\alpha}$ has a superpolynomial number of preimage right queries $\tilde{\boldsymbol{\alpha}}$ then either E succee s in extracting $\tilde{m}$ or M can be use to break the hi ing of $\langle \mathrm{C}, \mathrm{R} \rangle$. The proof is technical; at this point we give only some intuition which speaks to the truth of Claim 8. Full etails can be foun in Section 5.3. If there are superpolynomially many $\tilde{\boldsymbol{\alpha}}$ such that $\mathrm{M}(\tilde{\boldsymbol{\alpha}}) = \boldsymbol{\alpha}$, the chances that M can use C's response by itself to answer $\tilde{\boldsymbol{\alpha}}$ are negligible. It follows that either M must be content to not answer most of the $\tilde{\boldsymbol{\alpha}}$ such that $\mathrm{M}(\tilde{\boldsymbol{\alpha}}) = \boldsymbol{\alpha}$ (the probability of which can be boun e using a straightforwar con itional probability argument) or M must know some "extra information" about the $\tilde{f}_i$ which allows him to provi e a correct response to $\tilde{\boldsymbol{\alpha}}$. But this means that either M will use this extra information to correctly answer $\tilde{\boldsymbol{\alpha}}$ even when given a ran om answer to $\boldsymbol{\alpha}$ on the left (in which case E succee s in extracting $\tilde{m}$), or M is choosing to utilize this extra information only when C answers correctly on the left. However, the hi ing of the commitment in the first message ensures that M cannot *know* whether he receives correct responses on the left or not, an this ifference in behavior will allow us to use M to break hi ing.

Arme with Claim 8, we can now make efinitive statements about UNBAL an 1−2. For example, if UNBAL occurs then $\alpha_{i'}$ is epen ent on $\tilde{\alpha}_i$ for some $i' > i$, an so if R asks a new right challenge with the same i−th query, M will fix $\alpha_{i'}$ on the left. However, as $i' > i$, $\alpha_{i'}$ is rawn from a much larger challenge space than $\tilde{\alpha}_i$, an so M is "wasting challenge space". Specifically, the resi ual right challenge space with the i−th query fixe to $\tilde{\alpha}_i$ is superpolynomially larger than the resi ual left challenge space with $\alpha_{i'}$ fixe , an so with high probability, we will fin ourselves in a situation where the left query has superpolynomially many right query preimages. By Claim 8, this must not happen except with negligible probability. This simple combinatorial argument is essentially the content of Claim 5. In Section 5.2 we prove Claims 5 through 7 which show that if either UNBAL or 1−2 or "not (UNBAL or 1−2 or IND)" occur, then the left query will have superpolynomially many right query preimages. The proofs of Claims 6 an 7 are more involve than that of Claim 5, but they are still purely combinatorial.

Finally, we prove in Claim 9 that IND cannot happen using another re uction to hi ing. It uses the same framework as Claim 8 an has similar un erlying intuition (again, we iffer the technical iscussion an formal proof to Section 5.3). Here the main point is that if IND occurs then there exists a right query $\tilde{\alpha}_i$ on which no $\alpha_{i'}$ on the left is epen ent. Intuitively this means that M oes not nee any of the left challenges in or er to correctly return $\tilde{f}_i(\tilde{\alpha}_i)$, implying that he knows some information about the polynomial $\tilde{f}_i$. As in the intuition for Claim 8 this means either that extraction is successful, or that M is breaking hi ing.

5.2 Analyzing Dependencies

In Section 4.2, we looke at the commitment message of $\langle \mathrm{C}, \mathrm{R} \rangle$, an establishe that it suffices to consi er only transcripts $\mathbb{T} \in \mathsf{TRB}$ in or er to prove Theorem 1. We now consi er the query message of $\langle \mathrm{C}, \mathrm{R} \rangle$. Let R an L be the sets of right an left query vectors respectively. In this section we will often fix a commitment message $\mathbf{Com}$ (implicitly fixing $\tilde{\mathbf{Com}} = \mathrm{M}(\mathbf{Com})$) in which case M can be thought of as a eterministic function $\mathrm{M} : R \to L$ mapping $\tilde{\boldsymbol{\alpha}}$ to $\boldsymbol{\alpha}$. In the rest of this section we will frequently consi er subsets of R an L. Whenever we o so, we assume that $\mathbf{Com}$ is fixe (even if o not mention it explicitly). This is because we are really intereste in how M behaves on these subsets, an M is not efine as a function until $\mathbf{Com}$ is fixe .

De nition 8 (Honest Q eries). *For fixed* $\mathbf{Com}$*, we say that a right query vector* $\tilde{\boldsymbol{\alpha}} \in R$ *is* honest *if* M *answers* $\tilde{\boldsymbol{\alpha}}$ *honestly in the right interaction given correct responses to its queries* $\boldsymbol{\alpha} = \mathrm{M}(\tilde{\boldsymbol{\alpha}})$ *in the left interaction. We denote the set of honest right query vectors by* $\mathsf{HON}_{\mathbf{Com}}$*, or just* HON *when* $\mathbf{Com}$ *is clear from context.*

Let $R^i(\tilde{\alpha}_i)$ an $L^{i'}(\alpha_{i'})$ enote the sets of right an left query vectors whose $i-$th an $i'-$th coor inates are fixe on $\tilde{\alpha}_i$ an $\alpha_{i'}$, respectively. We write $\mathrm{M} : R^i_\tau(\tilde{\alpha}_i) \longrightarrow L^{i'}(\alpha_{i'})$ if M maps a $\tau-$fraction of $R^i(\tilde{\alpha}_i)$ to $L^{i'}(\alpha_{i'})$. Similarly, efine $\mathsf{HON}^i(\tilde{\alpha}_i) := R^i(\tilde{\alpha}_i) \cap \mathsf{HON}$. Finally, we write $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}(\cdots)$ as shorthan for $\Pr_{\tilde{\boldsymbol{\alpha}}}(\cdots | \tilde{\boldsymbol{\alpha}} \in \mathsf{HON})$.

Claim 4. *Let* $\mathbf{Com}$ *be the prefix of a transcript* $\mathbb{T} \in \mathsf{USEFUL}$*. Then*

. $|\mathsf{HON}| \geq \delta p^2 |R|$;

. *for any* $i \in [n]$*, if we (temporarily) define* $Z^i_\tau = \{\tilde{\alpha}_i \in [2^{\tilde{t}_i}] : |\mathsf{HON}^i(\tilde{\alpha}_i)| \leq \tau |R^i(\tilde{\alpha}_i)|\}$*, then*

$$\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}(\tilde{\alpha}_i \in Z^i_\tau) \leq \frac{\tau}{\delta p^2}.$$

Intuitively, 2 says that with goo probability, for all values $\tilde{\alpha}_i$ which appear in an honest $\tilde{\boldsymbol{\alpha}}$, $\mathsf{HON}^i(\tilde{\alpha}_i)$ comprises at least a $\tau-$fraction of $R^i(\tilde{\alpha}_i)$.

Proof. 1 follows imme iately from the efinition of USEFUL. For 2, we have

$$\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}(\tilde{\alpha}_i \in Z^i_\tau) \leq \frac{\Pr_{\tilde{\boldsymbol{\alpha}}}(\tilde{\boldsymbol{\alpha}} \in \mathsf{HON} | \tilde{\alpha}_i \in Z^i_\tau)}{\Pr_{\tilde{\boldsymbol{\alpha}}}(\tilde{\boldsymbol{\alpha}} \in \mathsf{HON})} \leq \frac{\tau}{\delta p^2}$$

□

Parameters. We have alrea y intro uce parameters $n = \mathcal{O}(\lambda)$, non-negligible $p = p(\lambda)$, constants $\delta, \delta' < 1/3$, an $\varepsilon^* = \big(\lambda/N\big)^{1/2}$ for $N = \mathrm{poly}(\lambda)$, a yet unspecifie polynomial. Shortly we will intro uce the values $\varepsilon = 1/n - \varepsilon'$ where $\varepsilon' = 1/2n^2$. We will require that $\varepsilon^* \leq \sigma\delta^2p^5/16$ an also that $\varepsilon^* \leq n\varepsilon'(\varepsilon'\delta\delta'p^3)^2/2048$, where $\sigma = \varepsilon'(\delta')^2p^4/257n^3$ is efine for convenience. All in all, setting $N = \omega\big(\lambda n^{10}p^{-18}\big)$ will suffice. We stress that there is no reason to believe that N must be such a large polynomial; it arises ue to our analysis, which is not concerne with minimizing N. We now formally efine $\varepsilon-$ epen ence.

De nition 9 (**$\varepsilon-$dependence**)**.** *For fixed $\mathbb{T} \in \mathsf{ACC}$ and $i, i' \in \{1, \ldots, n\}$, we say $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$ if $\Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\beta_{i'} = \alpha_{i'} \big| \tilde{\beta}_i = \tilde{\alpha}_i\big) \geq \varepsilon$.*

We stress that it is important to con ition on the event $\tilde{\boldsymbol{\beta}} \in \mathsf{HON}$ because any statement about M's behavior uring the query/response phase is useless unless M actually plans to successfully complete the right protocol.

Note that if $\varepsilon > \varepsilon'$ an $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$, then $\alpha_{i'}$ is automatically also $\varepsilon'-$ epen ent on $\tilde{\alpha}_i$. A itionally, notice that though our efinition oes leave open the possibility that there coul be more than one value which is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$, there can only be polynomially many (at most ε^{-1} to be exact). We call these values the *$\varepsilon-$dependencies* of $\tilde{\alpha}_i$. This notion is ifferent from $\varepsilon-$ epen ence efine above only because the $\varepsilon-$ epen encies exist regar less of what queries are aske in $\mathbb{T}$, whereas we only say that $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$ if both $\tilde{\alpha}_i$ an $\alpha_{i'}$ appear in $\mathbb{T}$. For the remain er of the proof we fix non-negligible values ε an ε' such that $\varepsilon = 1/n - \varepsilon'$ an $\varepsilon' = 1/2n^2$.

De nition 10 (**Special Sets of Transcripts**)**.** *Fix (as a function of λ), $\omega = \omega(1)$. Define the following sets of transcripts:*

. $\mathsf{UNBAL} := \big\{\mathbb{T} \in \mathsf{ACC} : \exists\ i' > i\ \mathit{st}\ \alpha_{i'}\ \mathit{is}\ \varepsilon' - \mathit{dependent\ on}\ \tilde{\alpha}_i\big\}$;

. $1{-}2 := \big\{\mathbb{T} \in \mathsf{ACC} : \exists\ (i_1, i_2, i')\ \mathit{st}\ \alpha_{i'}\ \mathit{is}\ \varepsilon' - \mathit{dependent\ on\ both}\ \tilde{\alpha}_{i_1}\ \mathit{and}\ \tilde{\alpha}_{i_2}\big\}$;

3. $\mathsf{IND} := \big\{\mathbb{T} \in \mathsf{ACC} : \exists\ i\ \mathit{st}\ \Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\beta_{i'} \neq \alpha_{i'}\ \forall\ i' \big| \tilde{\beta}_i = \tilde{\alpha}_i\big) \geq \varepsilon' n\big\}$;

4. $\mathsf{SUPER{-}POLY} := \big\{\mathbb{T} \in \mathsf{ACC} : {}^{\#}\{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON} : \mathrm{M}(\tilde{\boldsymbol{\alpha}}) = \boldsymbol{\alpha}\} \geq \lambda^{\omega}\big\}$.

Note that if $\mathbb{T} \notin \mathsf{IND}$ then for all i, there exists an i' such that $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$.

What follows is a sequence of claims which she s light on the relationships between the special sets of transcripts efine above. The statements all resemble one another an their proofs are similar, an are in or er of increasing complexity. We recommen those rea ers who are intereste in un erstan ing the proofs to rea them in or er as it will make the later ones much easier to un erstan . Rea ers who are intereste in un erstan ing the general flow of our overall proof will most likely fin rea ing the proof of Claim 5 an the statements of Claims 6 an 7 more than sufficient.

Claim 5. *Fix $\sigma = \frac{\varepsilon'(\delta')^2p^4}{257n^3}$. If $\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{UNBAL}\big) \geq \frac{\delta' p}{4}$, then*

$$\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \sigma.$$

Proof. We begin with the inequality $\Pr_{\mathbb{T}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{UNBAL}\big) \geq \delta' p^2/4$ (using the fact that $\Pr_{\mathbb{T}}(\mathbb{T} \in \mathsf{ACC}) \geq p$). Fix a ran om commit message **Com**. With probability at least $\delta' p^2/8$

over **Com**, we have that $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{UNBAL} \big| \mathbf{Com}\big) \geq \delta' p^2/8$. Now let $i' > i$ be such that $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\alpha_{i'}$ is $\varepsilon'-$ epen ent on $\tilde{\alpha}_i$ & $\mathbb{T} \in \mathsf{TRB} \big| \mathbf{Com}\big) \geq \delta' p^2/8n^2$. Such (i, i') must exist by efinition of UNBAL. Temporarily efine the sets X an Z as follows:

- $X = \big\{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON} : \alpha_{i'}$ is $\varepsilon'-$ epen ent on $\tilde{\alpha}_i$ & $\mathbb{T} \in \mathsf{TRB}\big\}$;
- $Z = \big\{\tilde{\alpha}_i \in \big[2^{\tilde{t}_i}\big] : \big|\mathsf{HON}^i(\tilde{\alpha}_i)\big| \leq \tau \big|R^i(\tilde{\alpha}_i)\big|\big\}$, where $\tau = \frac{\delta\delta' p^4}{16n^2}$.

Remark. Defining temporary sets X, Y an Z will be a recurring theme throughout the proofs in this section (though in this first proof we only nee X an Z). X will be a set of queries which isplay evi ence of a particular type of query epen ence; an Y an Z will be sets of queries in a particular coor inate in the right session which isplay some certain ba behavior. We will lower boun the probability that $\tilde{\boldsymbol{\alpha}} \in X$ using the claim's hypotheses, an we will upper boun the probability that $\tilde{\alpha}_i \in Z$ using Claim 4 (in fact, Z is the same set as Z^i_τ in the statement of Claim 4, just with the in ices omitte for simplicity). Though it oesn't appear here, we will also upper boun the probability that $\tilde{\alpha}_i \in Y$ using simple con itional probability. We now procee .

We have

$$\begin{aligned}\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X \text{ \& } \tilde{\alpha}_i \notin Z\big) &\geq \Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X\big) - \Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\alpha}_i \in Z\big) \\ &\geq \frac{\delta' p^2}{8n^2} - \frac{\delta' p^2}{16n^2} = \frac{\delta' p^2}{16n^2},\end{aligned}$$

using Claim 4. However, if $\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}$ is such that $\tilde{\boldsymbol{\alpha}} \in X$ & $\tilde{\alpha}_i \notin Z$, then $\mathbb{T} \in \mathsf{TRB}$ an M maps an $\varepsilon'-$fraction of $\mathsf{HON}^i(\tilde{\alpha}_i)$ into $L^{i'}(\alpha_{i'})$. Furthermore, as

$$\big|\mathsf{HON}^i(\tilde{\alpha}_i)\big| \geq \tau\big|R^i(\tilde{\alpha}_i)\big| \geq \tau 2^{\omega(\log\lambda)}\big|L^{i'}(\alpha_{i'})\big|$$

(using $i' > i$ an that the tags are well space), we see that M, when restricte appropriately, is superpolynomially many to one on average. This means that $\mathbb{T} \in \mathsf{TRB}$ an that $\boldsymbol{\alpha}$ has superpolynomially many preimages in HON whp, an so

$$\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \frac{\delta' p^2}{8} \cdot \frac{\delta' p^2}{16n^2} \cdot \big(1 - \mathbf{negl}(\lambda)\big) = \frac{(\delta')^2 p^4}{128n^2} - \mathbf{negl}(\lambda) > \sigma.$$

$\square$

Claim 6. *Fix* $\sigma = \frac{\varepsilon'(\delta')^2 p^4}{257n^3}$. *If* $\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap 1{-}2\big) \geq \frac{\delta' p}{4}$, *then*

$$\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \sigma.$$

Proof. Fix a commitment message **Com**. With probability at least $\delta' p^2/8$ over the choice of **Com**, we have $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\mathbb{T} \in \mathsf{TRB} \cap 1{-}2 \big| \mathbf{Com}\big) \geq \delta' p^2/8$. Let (i_1, i_2, i') be such that

$$\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\alpha_{i'} \text{ is } \varepsilon'- \text{ epen ent on } \tilde{\alpha}_{i_1} \text{ an } \tilde{\alpha}_{i_2} \text{ \& } \mathbb{T} \in \mathsf{TRB} \big| \mathbf{Com}\big) \geq \frac{\delta' p^2}{8n^3}.$$

Such (i_1, i_2, i') must exist by efinition of $1{-}2$. Temporarily efine sets X, Y an Z:

- $X = \big\{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON} : \alpha_{i'}$ is $\varepsilon'-$ epen ent on both $\tilde{\alpha}_{i_1}$ an $\tilde{\alpha}_{i_2}$ & $\mathbb{T} \in \mathsf{TRB}\big\}$;
- $Y = \big\{\tilde{\alpha}_{i_1} \in \big[2^{\tilde{t}_{i_1}}\big] : \Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\boldsymbol{\alpha} \in X \big| (\mathbf{Com}, \tilde{\alpha}_{i_1})\big) \leq \frac{\varepsilon'\delta' p^2}{16n^3}\big\}$;

- $Z = \{\tilde{\alpha}_{i_1} \in [2^{\tilde{t}_{i_1}}] : |\mathsf{HON}^{i_1}(\tilde{\alpha}_{i_1})| \leq \tau |R^{i_1}(\tilde{\alpha}_{i_1})|\}$, where $\tau = \frac{\varepsilon'\delta\delta' p^4}{32n^3}$.

Note that with **Com** fixe as above we have

$$\mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X\big) \geq \frac{\delta' p^2}{8n^3};\ \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\tilde{\alpha}_{i_1} \in Y \big| \tilde{\boldsymbol{\alpha}} \in X\big) \leq \frac{\varepsilon'}{2};\ \text{an }\ \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\alpha}_{i_1} \in Z\big) \leq \frac{\varepsilon'\delta' p^2}{32n^3}.$$

Now, for $v \in [2^{t_{i'}}]$, let $\mathbf{E}_v$ be the event "$\alpha_{i'} = v$." Note that if $\mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\mathbf{E}_v \big| \tilde{\boldsymbol{\alpha}} \in X\big) > 0$ then v is an $\varepsilon'-$ epen ency of $\tilde{\alpha}_{i_1}$. Let $D^{i'}(\tilde{\alpha}_{i_1}) \subset [2^{t_{i'}}]$ be the set of all $\varepsilon'-$ epen encies of $\tilde{\alpha}_{i_1}$. Then for fixe $\tilde{\alpha}_{i_1}$, we efine a probability mass function on $D^{i'}(\tilde{\alpha}_{i_1})$ by $P(v) = \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\mathbf{E}_v \big| \tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\alpha}_{i_1}\big)$. We say that $v^* \in D^{i'}(\tilde{\alpha}_{i_1})$ is *maximal* if $P(v^*) \geq P(v)$ for all $v \in D^{i'}(\tilde{\alpha}_{i_1})$. Clearly for a ran om $\tilde{\boldsymbol{\alpha}} \in X$, the resulting $\alpha_{i'}$ is maximal with probability at least ε' as $|D^{i'}(\tilde{\alpha}_{i_1})| \leq (\varepsilon')^{-1}$. We now lower boun the quantity $V = \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\alpha}_{i_1} \notin Y \cup Z \ \&\ \alpha_{i'} \text{ maximal}\big)$. We have

$$\begin{aligned}
V &\geq \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\alpha}_{i_1} \notin Y \ \&\ \alpha_{i'} \text{ maximal}\big) - \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\alpha}_{i_1} \in Z\big) \\
&\geq \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X\big) \cdot \Big[\mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\tilde{\alpha}_{i_1} \notin Y \ \&\ \alpha_{i'} \text{ maximal} \big| \tilde{\boldsymbol{\alpha}} \in X\big)\Big] - \frac{\varepsilon'\delta' p^2}{32n^3} \\
&\geq \frac{\delta' p^2}{8n^3} \cdot \Big[\mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\alpha_{i'} \text{ maximal} \big| \tilde{\boldsymbol{\alpha}} \in X\big) - \mathrm{Pr}_{\tilde{\boldsymbol{\alpha}}}\big(\tilde{\alpha}_{i_1} \in Y \big| \tilde{\boldsymbol{\alpha}} \in X\big)\Big] - \frac{\varepsilon'\delta' p^2}{32n^3} \\
&\geq \frac{\delta' p^2}{8n^3} \cdot \frac{\varepsilon'}{2} - \frac{\varepsilon'\delta' p^2}{32n^3} = \frac{\varepsilon'\delta' p^2}{32n^3}.
\end{aligned}$$

Finally we show that if $\tilde{\boldsymbol{\alpha}}$ is such that "$\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\alpha}_{i_1} \notin Y \cup Z \ \&\ \alpha_{i'}$ is maximal", then $\mathbb{T} \in \mathsf{TRB}$ (where $\mathbb{T}$ is the transcript resulting from $\tilde{\boldsymbol{\alpha}}$) an with probability at least $\tau' = \delta(\delta')^2(\varepsilon')^4 p^6/512n^6$ over $\tilde{\boldsymbol{\beta}} \in \mathsf{HON}$, we will have $\beta_{i'} = \alpha_{i'}$. This completes the proof of Claim 6 as it means that M maps a $\tau'-$fraction of HON into $L^{i'}(\alpha_{i'})$ an since

$$|\mathsf{HON}| \geq \delta p^2 |R| \geq \delta p^2 2^{\omega(\log \lambda)} |L^{i'}(\alpha_{i'})|$$

(using the "well space " property of the tags), M is superpolynomially many to one on average when restricte appropriately. Just like in the proof of Claim 5, this gives

$$\mathrm{Pr}_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \frac{\delta' p^2}{8} \cdot \frac{\varepsilon'\delta' p^2}{32n^3} - \mathbf{negl}(\lambda) > \sigma.$$

So all that remains is to prove that if $\tilde{\boldsymbol{\alpha}}$ is such that "$\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\alpha}_{i_1} \notin Y \cup Z \ \&\ \alpha_{i'}$ is maximal" then $\mathrm{Pr}_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\beta_{i'} = \alpha_{i'}\big) \geq \tau'$. The maximality of $\alpha_{i'}$ combine with the fact that $\tilde{\alpha}_{i_1} \notin Y$ ensure that if $\tilde{\boldsymbol{\gamma}} \in \mathsf{HON}^{i_1}(\tilde{\alpha}_{i_1})$ is chosen at ran om, then with probability at least $(\varepsilon')^2\delta' p^2/16n^3$ over $\tilde{\boldsymbol{\gamma}}$ we will have "$\gamma_{i'}$ is $\varepsilon' -$ epen ent on $\tilde{\gamma}_{i_1}$ an $\tilde{\gamma}_{i_2}$ & $\gamma_{i'} = \alpha_{i'}$". Moreover, as $\tilde{\alpha}_{i_1} \notin Z$, a ran om $\tilde{\boldsymbol{\gamma}} \in R^{i_1}(\tilde{\alpha}_{i_1})$ will be such that "$\gamma_{i'}$ is $\varepsilon' -$ epen ent on $\tilde{\gamma}_{i_1}$ an $\tilde{\gamma}_{i_2}$ & $\gamma_{i'} = \alpha_{i'}$" with probability at least $\delta(\delta')^2(\varepsilon')^3 p^6/512n^6 = \tau'/\varepsilon'$.

So choose a ran om $\tilde{\boldsymbol{\gamma}} \in R^{i_1}(\tilde{\alpha}_{i_1})$ an then choose a ran om $\tilde{\boldsymbol{\beta}} \in \mathsf{HON}^{i_2}(\tilde{\gamma}_{i_2})$. Clearly such a $\tilde{\boldsymbol{\beta}}$ is a ran om element of HON. As "$\gamma_{i'}$ is $\varepsilon' -$ epen ent on $\tilde{\gamma}_{i_2}$ & $\gamma_{i'} = \alpha_{i'}$" with probability at least τ'/ε', the efinition of $\varepsilon'-$ epen ence ensures that $\beta_{i'} = \gamma_{i'} = \alpha_{i'}$ with probability at least τ', as esire . □

Claim 7. *Fix* $\sigma = \frac{\varepsilon'(\delta')^2 p^4}{257n^3}$. *If* $\mathrm{Pr}_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \setminus (\mathsf{UNBAL} \cup \mathsf{1{-}2} \cup \mathsf{IND})\big) \geq \frac{\delta' p}{4}$, *then*

$$\mathrm{Pr}_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \sigma.$$

Proof. Fix a commitment message **Com**. With probability at least $\delta' p^2/8$ over the choice of **Com**, we have $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\mathbb{T} \in \mathsf{TRB} \backslash (\mathsf{UNBAL} \cup 1{-}2 \cup \mathsf{IND}) \big| \mathbf{Com}\big) \geq \delta' p^2/8$. Now consi er the consequences of $\mathbb{T} \notin (\mathsf{UNBAL} \cup 1{-}2 \cup \mathsf{IND})$:

- if $\mathbb{T} \notin \mathsf{UNBAL}$, then for all $i' > i$, $\alpha_{i'}$ cannot be $\varepsilon-$ epen ent on $\tilde{\alpha}_i$ (since $\varepsilon \geq \varepsilon'$);
- if $\mathbb{T} \notin 1{-}2$, then there o not exist (i_1, i_2, i') such that $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_{i_1}$ an $\tilde{\alpha}_{i_2}$;
- if $\mathbb{T} \notin \mathsf{IND}$ then for every i, there exists at least one i' such that $\alpha_{i'}$ is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$.

It follows that if $\mathbb{T} \notin (\mathsf{UNBAL} \cup 1{-}2 \cup \mathsf{IND})$ then for each i, α_i must be $\varepsilon-$ epen ent on $\tilde{\alpha}_i$. In ee , α_1 must be $\varepsilon-$ epen ent on $\tilde{\alpha}_1$ as something must epen on $\tilde{\alpha}_1$ an it cannot be $\alpha_{i'}$ for $i' > 1$. Next, either α_1 or α_2 must be $\varepsilon-$ epen ent on $\tilde{\alpha}_2$ an it cannot be α_1 as that is alrea y epen ent on $\tilde{\alpha}_1$. Continuing in this fashion, we e uce that each α_i is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$.

Now, going one step further in examining the consequences of $\mathbb{T} \notin (\mathsf{UNBAL} \cup 1{-}2 \cup \mathsf{IND})$, since each α_i is $\varepsilon-$ epen ent on $\tilde{\alpha}_i$ an $\mathbb{T} \notin 1{-}2$, it must be that $\alpha_{i'}$ is not $\varepsilon'-$ epen ent on $\tilde{\alpha}_i$ for all $i' \neq i$. It follows that for all i, $\Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\exists\, i' \neq i \text{ st } \beta_{i'} = \alpha_{i'} \big| \tilde{\beta}_i = \tilde{\alpha}_i\big) \leq \varepsilon' n$. As $\mathbb{T} \notin \mathsf{IND}$, we have that for all i,

$$
\begin{aligned}
\Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\beta_i = \alpha_i \big| \tilde{\beta}_i = \tilde{\alpha}_i\big) \quad &\geq \quad \Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\exists\, i' \text{ st } \beta_{i'} = \alpha_{i'} \big| \tilde{\beta}_i = \tilde{\alpha}_i\big) \\
&- \quad \Pr_{\tilde{\boldsymbol{\beta}} \in \mathsf{HON}}\big(\exists\, i' \neq i \text{ st } \beta_{i'} = \alpha_{i'} \big| \tilde{\beta}_i = \tilde{\alpha}_i\big). \\
&\geq \quad 1 - \varepsilon' n - \varepsilon' n = 1 - 2\varepsilon' n,
\end{aligned}
$$

so we see that, in fact, each α_i is $(1 - 2\varepsilon' n)-$ epen ent on $\tilde{\alpha}_i$. As $2\varepsilon' n < \frac{1}{2}$, each $\tilde{\alpha}_i$ has a unique $(1 - 2\varepsilon' n)-$ epencence.

Now, choose a ran om $\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}$ an let $S = \{i \in [n] : \tilde{t}_i \leq t_i\}$, $\tilde{\boldsymbol{\alpha}}_S = (\tilde{\alpha}_i)_{i \in S}$ an efine $\mathsf{HON}^S(\tilde{\boldsymbol{\alpha}}_S) = \bigcap_{i \in S} \mathsf{HON}^i(\tilde{\alpha}_i)$. Define $R^S(\tilde{\boldsymbol{\alpha}}_S)$ an $L^S(\boldsymbol{\alpha}_S)$ similarly. Now, temporarily efine sets X, Y, Z as follows:

- $X = \big\{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON} : \alpha_i \text{ is } (1 - 2\varepsilon' n) - \text{ epen ent on } \tilde{\alpha}_i \ \forall\, i \ \&\ \mathbb{T} \in \mathsf{TRB}\big\}$;
- $Y = \big\{\tilde{\boldsymbol{\alpha}}_S : \Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X \big| \tilde{\boldsymbol{\alpha}}_S\big) \leq \frac{\delta' p^2}{16}\big\}$;
- $Z = \big\{\tilde{\boldsymbol{\alpha}}_S : \big|\mathsf{HON}^S(\tilde{\boldsymbol{\alpha}}_S)\big| \leq \tau \big|R^S(\tilde{\boldsymbol{\alpha}}_S)\big|\big\}$, where $\tau = \frac{\delta \delta' p^4}{32}$.

Note that

$$
\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X\big) \geq \frac{\delta' p^2}{8}; \ \Pr_{\tilde{\boldsymbol{\alpha}}}\big(\tilde{\boldsymbol{\alpha}}_S \in Y \big| \tilde{\boldsymbol{\alpha}} \in X\big) \leq \frac{1}{2}; \text{ an } \ \Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}}_S \in Z\big) \leq \frac{\delta' p^2}{32},
$$

an so $\Pr_{\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}}\big(\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\boldsymbol{\alpha}}_S \notin Y \cup Z\big) \geq \delta' p^2/32$. Now suppose that some $\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}$ is such that "$\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\boldsymbol{\alpha}}_S \notin Y \cup Z$". Then $\mathbb{T} \in \mathsf{TRB}$ an for a ran omly selecte $\tilde{\boldsymbol{\beta}} \in \mathsf{HON}^S(\tilde{\boldsymbol{\alpha}}_S)$, $\tilde{\boldsymbol{\beta}} \in X$ with probability at least $\delta' p^2/16$. But if $\tilde{\boldsymbol{\alpha}}, \tilde{\boldsymbol{\beta}} \in X$ an $\tilde{\boldsymbol{\alpha}}_S = \tilde{\boldsymbol{\beta}}_S$, then $\boldsymbol{\alpha}_S = \boldsymbol{\beta}_S$. In ee , all $\tilde{\alpha}_i$ have a unique $(1 - 2\varepsilon' n)-$ epen ency, meaning that if α_i an β_i are epen ent on $\tilde{\alpha}_i$ an $\tilde{\beta}_i$ an $\tilde{\alpha}_i = \tilde{\beta}_i$ for all $i \in S$, then it must be that $\alpha_i = \beta_i$ for all $i \in S$.

It follows that if "$\tilde{\boldsymbol{\alpha}} \in X \ \&\ \tilde{\boldsymbol{\alpha}}_S \notin Y \cup Z$" then $\mathbb{T} \in \mathsf{TRB}$ an M maps a $\tau'-$fraction of $\mathsf{HON}^S(\tilde{\boldsymbol{\alpha}}_S)$ into $L^S(\boldsymbol{\alpha}_S)$ where $\tau' = \delta' p^2/16$. Moreover,

$$
\big|\mathsf{HON}^S(\tilde{\boldsymbol{\alpha}}_S)\big| \geq \tau \big|R^S(\tilde{\boldsymbol{\alpha}}_S)\big| \geq \tau 2^{\omega(\log \lambda)} \big|L^S(\boldsymbol{\alpha}_S)\big|
$$

(using the "goo istance an balance" property of the tags). As in the proofs of Claims 5 an 6, we have

$$\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \frac{\delta' p^2}{8} \cdot \frac{\delta' p^2}{32} - \mathbf{negl}(\lambda) > \sigma.$$

□

5.3 Reductions to the Hiding of $\langle \mathrm{C}, \mathrm{R}\rangle$

In this section we complete the proof of Lemma 1 by proving two claims which show how to use an M with unlikely behavior to break the hi ing of $\langle \mathrm{C}, \mathrm{R}\rangle$. We first give an intuitive escription of our metho of argument. This escription is slightly technical but oes not get into the specifics of either Claim 8 or Claim 9.

We construct an a versary $\mathcal{A}$ who takes part in the hi ing game for $\langle \mathrm{C}, \mathrm{R}\rangle$. $\mathcal{A}$ is efine as follows:

- $\mathcal{A}$ chooses ran om $m_0, m_1 \in \mathbb{Z}_q$ an sen s (m_0, m_1) to a challenger $\mathcal{C}$, signaling the beginning of the hi ing game of $\langle \mathrm{C}, \mathrm{R}\rangle$.
- $\mathcal{A}$ instantiates M an runs two sessions of $\langle \mathrm{C}, \mathrm{R}\rangle$ until the en of the commit phase of both executions, forwar ing the messages it receives as C to $\mathcal{C}$. In the left execution, $\mathcal{C}$ commits to m_u for secret $u \in \{0, 1\}$. More specifically:
  - $\mathcal{A}$, acting as R, sen s $\tilde{\sigma}$ to M, an receives σ which it forwar s to $\mathcal{C}$.
  - $\mathcal{A}$ then receives $\mathbf{Com}$ from $\mathcal{C}$ which it forwar s to M, an receives $\tilde{\mathbf{Com}}$.
  - $\mathcal{A}$ sen s ran om $\tilde{\boldsymbol{\alpha}}$ such that $\tilde{\alpha}_i \in \big[2^{\tilde{t}_i}\big]$ to M, receiveing $\boldsymbol{\alpha}$ which it forwar s to $\mathcal{C}$.
  - $\mathcal{A}$ receives $\mathbf{a}$ from $\mathcal{C}$ which it forwar s to M, obtaining $\tilde{\mathbf{a}}$.
  - $\mathcal{A}$ continues forwar ing messages between M an $\mathcal{C}$ uring the zero-knowle ge proof phase of $\langle \mathrm{C}, \mathrm{R}\rangle$, playing honestly as R in the right interaction.
  - When the proofs are finishe , $\mathcal{A}$ verifies both π an $\tilde{\pi}$. If either is not accepte , $\mathcal{A}$ aborts. Let $\mathbb{T} = \big(\mathbf{Com}, \tilde{\boldsymbol{\alpha}}, \mathbf{a}\big)$ be the resulting transcript.
- $\mathcal{A}$ chooses ran om $u' \in \{0, 1\}$ an   efines polynomial vector $\mathbf{f}$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{a}$ an every coor inate of $\mathbf{f}$ has constant term $m_{u'}$.
- $\mathcal{A}$ rewin s M to the beginning of the query phase of the right execution an sen s a new query $\tilde{\boldsymbol{\beta}}$, receiving left query $\boldsymbol{\beta}$. It can o this many times, resulting in a set of new right queries $\{\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}, \dots\}$.
- $\mathcal{A}$ answers the left queries it obtaine in the previous step with $\mathbf{f}$, an receives a right response. It collects the points it receives on the right into the set $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}}), \dots\big\}$.
- $\mathcal{A}$ tests whether the points $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}}), \dots\big\}$ satisfy some con ition. If so, then $\mathcal{A}$ outputs u', if not it outputs $1 - u'$.

Exactly what con ition $\mathcal{A}$ tests for will change between the two proofs. In the proof of Claim 8, $\mathcal{A}$ checks that the points $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ are collinear, while in the proof of Claim 9, $\mathcal{A}$ checks that $\tilde{b}_i = \tilde{a}_i$ for some preselecte i. The important thing however, is that the con ition be satisfie when M answers correctly, but not when M answers incorrectly. Note that if $u' = u$ then responses generate with $\mathbf{f}$ are correct an so if $\mathbb{T} \in \mathsf{USEFUL}$, then we can lower boun the probability that M answers correctly on the right using Claim 4. On the other han , if $u' \neq u$ then the responses on the left are ran om. If $\mathbb{T} \notin \mathsf{EXT}$ then we have an upper boun on the probability that M answers any right query correctly. These observations together tell us that there is a non-negligible gap between the probability that the con ition is satisfie when $u' = u$ an when $u' \neq u$. This gap translates to $\mathcal{A}$ having a noticeable a vantage in winning the hi ing game.

There are two main issues with the above outline which nee to be a resse . We iscuss them informally here in or er to exhibit the ifficulties face when trying to push the above intuition through. The first is that we have assume that $\mathbb{T} \in \mathsf{TRB}$ when in reality we are only allowe to assume that $\mathbb{T} \in \mathsf{TRB}$ with probability at least $\frac{\delta' p}{4}$. Fact 1 below says essentially that if the gap between the con ition being satisfie when $u' = u$ an not when $u' \neq u$ is large enough, this oes not matter.

A secon , more subtle, issue is that we can only use $\mathbb{T} \notin \mathsf{EXT}$ to upper boun the probability that M answers correctly on the right when $u' \neq u$ if the answers on the left are istribute as if they were answere by the extractor, E. Recall that E is instructe to answer ran omly on the left unless the left query is the same as in the main threa , in which case E reuses the main threa 's answer. Note that this process is exactly the same as answering one query accor ing to $\mathbf{f}$ when $u' \neq u$. However, if M is rewoun more than once an asks left challenges $\{\boldsymbol{\beta}, \boldsymbol{\gamma}\}$, the responses it receives will no longer be ran om. In ee , $\big\{(\boldsymbol{\alpha}, \mathbf{a}), (\boldsymbol{\beta}, \mathbf{b}), (\boldsymbol{\gamma}, \mathbf{c})\big\}$ will be collinear so certainly not ran om (an hence, not istribute as E's responses). This will mean, for example, that we will not be able to use Claim 1 to argue that M's responses on the right cannot be incorrect but collinear. In fact, if M receives ran om but collinear responses on the left, it might well be the case that M's right responses are incorrect but collinear (consi er for example the copying MIM). Instea , we will have to use the a itional hypothesis that $\mathbb{T} \in \mathsf{SUPER{-}POLY}$ along with the observation that $\boldsymbol{\beta}$ is answere i entically to how E woul answer it to boun the probability that $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ are collinear when $u' \neq u$. For etails see Claim 8 below.

In the proof of Claim 9, $\mathcal{A}$ rewin s M an asks a new challenge $\tilde{\boldsymbol{\beta}}$ such that $\tilde{\beta}_i = \tilde{\alpha}_i$ for some i. Note that if $\boldsymbol{\beta}$ is such that $\beta_{i'} = \alpha_{i'}$ for some i', then M will receive at least one correct answer on the left regar less of whether $u' = u$ or not. If $u' \neq u$, this will mean that the answers M receives on the left are not istribute i entically to the answers M woul receive from E. In ee , suppose that some $\alpha_{i'}$ is epen ent on $\tilde{\alpha}_i$. Then if $\tilde{\boldsymbol{\beta}}$ such that $\tilde{\beta}_i = \tilde{\alpha}_i$ is aske on the right by $\mathcal{A}$, M will ask $\boldsymbol{\beta}$ on the left with $\beta_{i'} = \alpha_{i'}$, an get at least one correct response. If, on the other han , $\tilde{\boldsymbol{\beta}}$ is aske on the right by E, then with overwhelming probability, $\tilde{\boldsymbol{\beta}}$ oes not share any query with the query vector aske in the main threa as E raws its queries ran omly, in epen ent of $\mathbb{T}$. This means that $\beta_{i'}$ will likely not equal $\alpha_{i'}$, an so M will get a ran om response instea of a correct one. This inherent ifference between $\mathcal{A}$ an E means that we cannot use Claim 2 to upper boun the probability that M answers correctly on the right. Instea we have to use the a itional assumption that $\mathbb{T} \notin \mathsf{IND}$ to ensure that $\boldsymbol{\beta}$ is completely istinct from $\boldsymbol{\alpha}$ *even though* $\tilde{\beta}_i = \tilde{\alpha}_i$ on the right. Even with this assumption, the proof requires some elicacy to ensure that in fact the answers $\mathcal{A}$ gives to M are the same as the ones E woul give. For etails see the proof of Claim 9.

Fact 1. *Consider an efficiently testable condition that the set* $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\boldsymbol{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\boldsymbol{c}}), \dots\big\}$ *either satisfies or not, as described in the above paragraphs. Let* $\mathbf{E}$ *be an event such that:*

- $\Pr_{\mathbb{T} \in \mathsf{ACC}}(\mathbf{E}) \geq \xi$;
- $\Pr\big(\text{Con ition satisfie } \big| u' = u \ \&\ \mathbf{E}\big) \geq \xi'$;

- $\Pr\big(\text{Con ition satisfie }\big|u' \neq u \ \&\ \mathbf{E}\big) \leq \xi''$,

for non-negligible values ξ, ξ', ξ'' satisfying $\xi'' \leq (p\xi\xi')/8$. Then there exists a PPT algorithm $\mathcal{A}$ that breaks the hiding of $\langle \mathrm{C}, \mathrm{R} \rangle$.

Proof. Fix $\ell = 1/2\xi''$ an let $\mathcal{A}$ play in an $\ell-$way version of the usual hi ing game of $\langle \mathrm{C}, \mathrm{R} \rangle$ as follows:

- $\mathcal{A}$ chooses ran om $m_1, \ldots, m_\ell \in \mathbb{Z}_q$ an sen s $(m_1, \ldots, m_\ell)$ to $\mathcal{C}$.
- $\mathcal{A}$ instantiates M an runs two sessions of $\langle \mathrm{C}, \mathrm{R} \rangle$ until the en of the commit phase of both executions, forwar ing the messages it receives as C to $\mathcal{C}$. In the left execution, $\mathcal{C}$ commits to $m_{j'}$ for secret $j' \in [\ell]$.
- For each $j \in [\ell]$, $\mathcal{A}$ efines polynomial vectors $\mathbf{g}_j$ such that $\mathbf{g}_j(\boldsymbol{\alpha}) = \mathbf{a}$ an every coor inate of $\mathbf{g}_j$ has constant term m_j.
- $\mathcal{A}$ rewin s M to the beginning of the query phase of the right execution an sen s new queries $\tilde{\boldsymbol{\beta}}, \tilde{\boldsymbol{\gamma}}, \ldots$, receiving left queries $\boldsymbol{\beta}, \boldsymbol{\gamma}, \ldots$.
- For each $j \in [\ell]$, $\mathcal{A}$ answers the left queries it obtaine in the previous step with $\mathbf{g}_j$, an receives a right response. It collects the set $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}_j), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}}_j), \ldots\big\}_{j \in [\ell]}$.
- For each $j \in [\ell]$, $\mathcal{A}$ tests whether the points $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}_j), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}}_j), \ldots\big\}$ satisfy the con ition. If so, then $\mathcal{A}$ outputs $j^* = j$ an halts.

Note that

$$\begin{aligned}
\Pr(j^* = j') \ &\geq\ \Pr_{\mathbb{T}}\big(\mathbb{T} \in \mathsf{ACC}\big) \cdot \Pr_{\mathbb{T} \in \mathsf{ACC}}(\mathbf{E}) \\
&\cdot\ \Pr\big(\text{Con ition satisfie when } j = j' \big| \mathbf{E}\big) \\
&\cdot\ \Pr\big(\text{Con ition not satisfie whenever } j \neq j' \big| \mathbf{E}\big) \\
&\geq\ (p\xi\xi') \cdot \Pr\big(\text{Not } \mathbf{E}'_j \text{ for all } j \neq j' \big| \mathbf{E}\big).
\end{aligned}$$

where $\mathbf{E}'_j$ is the event

$$\mathbf{E}'_j : \text{“Con itions are satisfie when } \mathbf{g}_j \text{ is use to answer left queries.”}$$

We are given that $\Pr\big(\mathbf{E}'_j \big| \mathbf{E}\big) \leq \xi''$ for all $j \neq j'$, an as the $\mathbf{E}'_j$ are in epen ent this means that the expecte number of $\mathbf{E}'_j$ which occur is at most $\xi''\ell = 1/2$. It follows that

$$\Pr(j^* = j') \geq (p\xi\xi') \cdot \Pr\big(\text{No } \mathbf{E}'_j \text{ occur when } j \neq j' \big| \mathbf{E}\big) \geq \frac{p\xi\xi'}{2} \geq \frac{2}{\ell},$$

which means that $\mathcal{A}$'s chances of winning the hi ing game are noticeably greater than $1/\ell$, violating the hi ing of $\langle \mathrm{C}, \mathrm{R} \rangle$. ☐

Claim 8. *Fix $\sigma = \frac{\varepsilon'(\delta')^2 p^4}{257 n^3}$. If $\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}\big) \geq \sigma$ then there exists a PPT algorithm $\mathcal{A}$ who breaks the hiding of $\langle \mathrm{C}, \mathrm{R} \rangle$.*

Proof. Our $\mathcal{A}$ procee s as follows.

- $\mathcal{A}$ chooses ran om $m_0, m_1 \in \mathbb{Z}_q$ an begins the hi ing game, sen ing (m_0, m_1) to $\mathcal{C}$. Then $\mathcal{A}$ instantiates M an runs two sessions of $\langle \mathrm{C}, \mathrm{R} \rangle$ forwar ing the messages it receives as C to $\mathcal{C}$. In the left interaction, $\mathcal{C}$ commits to m_u for unknown $u \in \{0,1\}$. Let $\mathbb{T} = \big(\mathbf{Com}, \tilde{\boldsymbol{\alpha}}, \mathbf{a}\big)$ be the resulting transcript. A itionally, $\mathcal{A}$ chooses ran om $u' \in \{0,1\}$ an efines the polynomial vector $\mathbf{f}$, to be the unique such vector so that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{a}$ an so that every coor inate of $\mathbf{f}$ has constant term $m_{u'}$.

- $\mathcal{A}$ chooses two new ran om challenge vectors $\tilde{\boldsymbol{\beta}}$ an $\tilde{\boldsymbol{\gamma}}$ such that each $\tilde{\beta}_i, \tilde{\gamma}_i \in \big[2^{\tilde{t}_i}\big]$. It rewin s M back to the beginning of the right execution's query message an sen s $\tilde{\boldsymbol{\beta}}$, receiving left query $\boldsymbol{\beta}$. It respon s with $\mathbf{b} = \mathbf{f}(\boldsymbol{\beta})$ an receives right response $\tilde{\mathbf{b}}$. It repeats this process, sen ing challenge $\tilde{\boldsymbol{\gamma}}$, answering $\boldsymbol{\gamma}$ with $\mathbf{c} = \mathbf{f}(\boldsymbol{\gamma})$ an receiving $\tilde{\mathbf{c}}$.

- $\mathcal{A}$ checks whether the points $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ are collinear (by checking for collinearity in each coor inate). If so, $\mathcal{A}$ outputs u', if not $\mathcal{A}$ outputs $1 - u'$.

In light of Fact 1, it suffices to construct an event $\mathbf{E}$ such that:

1. $\Pr_{\mathbb{T} \in \mathsf{ACC}}\big(\mathbf{E}\big) \geq \sigma$;

2. $\Pr\Big(\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\} \text{ collinear}\big| u' = u \ \& \ \mathbf{E}\Big) \geq \delta^2 p^4$;

3. $\Pr\Big(\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\} \text{ collinear}\big| u' \neq u \ \& \ \mathbf{E}\Big) \leq 2\varepsilon^*$,

since $\varepsilon^* \leq \sigma\delta^2 p^5/16$. Let $\mathbf{E}$ (temporarily) be the event "$\mathbb{T} \in \mathsf{TRB} \cap \mathsf{SUPER{-}POLY}$." By hypothesis of Claim 8, $\Pr_{\mathbb{T} \in \mathsf{ACC}}(\mathbf{E}) \geq \sigma$. Also, if $\mathbb{T} \in \mathsf{USEFUL}$ an $u' = u$ then Claim 4 ensures that M answers $\tilde{\boldsymbol{\beta}}$ an $\tilde{\boldsymbol{\gamma}}$ correctly on the right with probability at least $(\delta p^2)^2$, which means that the probability that $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ are collinear given $u' = u$ & $\mathbf{E}$ is at least as high. On the other han ,

$$\begin{aligned}
\Pr\Big(\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\} \text{ collinear}\big| u' \neq u \ \& \ \mathbf{E}\Big) &\leq \Pr\big(\text{collinear}\big|\tilde{\mathbf{b}} \text{ incorrect}\big) \\
&+ \Pr\big(\tilde{\mathbf{b}} \text{ correct}\big| u' \neq u \ \& \ \mathbf{E}\big) \\
&\leq \Pr\big(\text{collinear}\big|\tilde{\mathbf{b}} \text{ incorrect}\big) + \varepsilon^*,
\end{aligned}$$

as if $u' \neq u$ then the answer M receives to $\boldsymbol{\beta}$ is istribute i entically to the answer it woul have receive from E, an $\mathbb{T} \notin \mathsf{EXT}$. Therefore, it suffices to show that

$$\Pr\Big(\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\} \text{ collinear}\big|\tilde{\mathbf{b}} \text{ incorrect}\Big) = \mathbf{negl}(\lambda).$$

Suppose that $\tilde{\boldsymbol{\alpha}}, \tilde{\boldsymbol{\alpha}}' \in \mathsf{HON}$ are such that $\mathrm{M}(\tilde{\boldsymbol{\alpha}}) = \boldsymbol{\alpha} = \mathrm{M}(\tilde{\boldsymbol{\alpha}}')$. Note that it cannot be the case that $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ an $\big\{(\tilde{\boldsymbol{\alpha}}', \tilde{\mathbf{a}}'), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\gamma}, \tilde{\mathbf{c}})\big\}$ are collinear as this woul mean that the four points

$$\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\alpha}}', \tilde{\mathbf{a}}'), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$$

lie on the same line, an moreover, that this is the correct line as it contains the correct points $(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}})$ an $(\tilde{\boldsymbol{\alpha}}', \tilde{\mathbf{a}}')$. This contra icts the hypothesis that $\tilde{\mathbf{b}}$ is an incorrect answer. So we see that there exists at most one $\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}$ such that

1. $\mathrm{M}(\tilde{\boldsymbol{\alpha}}) = \boldsymbol{\alpha}$;

2. $\big\{(\tilde{\boldsymbol{\alpha}}, \tilde{\mathbf{a}}), (\tilde{\boldsymbol{\beta}}, \tilde{\mathbf{b}}), (\tilde{\boldsymbol{\gamma}}, \tilde{\mathbf{c}})\big\}$ are collinear.

As $\mathbb{T} \in \mathsf{SUPER{-}POLY}$, there are at least λ^ω values of $\tilde{\boldsymbol{\alpha}} \in \mathsf{HON}$ such that number 1 hol s, so the probability that $\mathcal{A}$ chose the unique $\tilde{\boldsymbol{\alpha}}$ such that both 1 an 2 hol is negligible. $\square$

Claim 9. *If* $\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{IND}\big)\geq\frac{\delta' p}{4}$ *then there exists a PPT algorithm $\mathcal{A}$ who breaks the hiding of* $\langle \mathrm{C},\mathrm{R}\rangle$.

Proof. For each $i'\in[n]$, efine the set

$$\mathsf{FIXED}^{i'}=\big\{\mathbf{Com}:\exists\ v\in\big[2^{t_{i'}}\big]\ \text{st}\ \Pr_{\tilde{\boldsymbol{\alpha}}\in\mathsf{HON}}\big(\alpha_{i'}=v\big|\mathbf{Com}\big)\geq\varepsilon\big\},$$

an let $\mathsf{FIXED}=\big\{\mathbb{T}\in\mathsf{ACC}:\mathbf{Com}\in\mathsf{FIXED}^{i'}\ \text{for some}\ i'\in[n]\big\}$.

Fact 2. *Fix* $\sigma=\frac{\varepsilon'(\delta')^2p^4}{257n^3}$. *If* $\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{FIXED}\big)\geq\frac{\delta' p}{8}$, *then*

$$\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{SUPER\!-\!POLY}\big)\geq\sigma.$$

Proof of Fact . This proof is similar to (an easier than) the proofs of Claims 5 through 7. Fix commitment message $\mathbf{Com}$. Just as in the previous proofs, with probability at least $\delta' p^2/16$ over $\mathbf{Com}$, $\Pr_{\tilde{\boldsymbol{\alpha}}\in\mathsf{HON}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{FIXED}\big|\mathbf{Com}\big)\geq\delta' p^2/16$. Let $i'\in[n]$ an $v\in\big[2^{t_{i'}}\big]$ be such that

$$\Pr_{\tilde{\boldsymbol{\alpha}}\in\mathsf{HON}}\big(\alpha_{i'}=v\ \&\ \mathbb{T}\in\mathsf{TRB}\big|\mathbf{Com}\big)\geq\frac{\varepsilon\delta' p^2}{16n}.$$

Such (i',v) must exist by efinition of FIXED. But this means that $\mathbb{T}\in\mathsf{TRB}$ an M maps at least a $\tau-$fraction of HON into $L^{i'}(v)$, where $\tau=\varepsilon\delta' p^2/16n$. As

$$\big|\mathsf{HON}\big|\geq\delta p^2\big|R\big|\geq\delta p^2 2^{\omega(\log\lambda)}\big|L^{i'}(v)\big|,$$

(using the "well space " property of the tags), we see that M, when restricte appropriately, is superpolynomially many to one on average. It follows that

$$\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{SUPER\!-\!POLY}\big)\geq\frac{\delta' p^2}{16}\cdot\frac{\varepsilon\delta' p^2}{16n}-\mathbf{negl}(\lambda)>\sigma.$$

□

In light of Fact 2 an Claim 8, it suffices to show that if $\Pr_{\tilde{\boldsymbol{\alpha}}\in\mathsf{HON}}\big(\mathbb{T}\in\mathsf{TRB}\cap\mathsf{IND}\backslash\mathsf{FIXED}\big)\geq\delta' p/8$ then there exists a PPT $\mathcal{A}$ who breaks the hi ing of $\langle \mathrm{C},\mathrm{R}\rangle$. Therefore, assume that this probability is at least $\delta' p/8$ an efine $\mathcal{A}$ as follows.

- $\mathcal{A}$ chooses ran om $m_0,m_1\in\mathbb{Z}_q$ an begins the hi ing game, sen ing (m_0,m_1) to $\mathcal{C}$. Then $\mathcal{A}$ instantiates M an runs two sessions of $\langle \mathrm{C},\mathrm{R}\rangle$ forwar ing the messages it receives as C to $\mathcal{C}$. In the left interaction, $\mathcal{C}$ commits to m_u for unknown $u\in\{0,1\}$. Let $\mathbb{T}=\big(\mathbf{Com},\tilde{\boldsymbol{\alpha}},\mathbf{a}\big)$ be the resulting transcript. A itionally, $\mathcal{A}$ chooses ran om $u'\in\{0,1\}$ an efines the polynomial vector $\mathbf{f}$, to be the unique such vector so that $\mathbf{f}(\boldsymbol{\alpha})=\mathbf{a}$ an so that every coor inate of $\mathbf{f}$ has constant term $m_{u'}$.
- $\mathcal{A}$ chooses ran om $i\in[n]$ an ran om legal challenge vector $\tilde{\boldsymbol{\beta}}$ such that $\tilde{\beta}_i=\tilde{\alpha}_i$. It rewin s M back to the beginning of the right execution's query message an sen s $\tilde{\boldsymbol{\beta}}$, receiving left query $\boldsymbol{\beta}$. If $\beta_{i'}=\alpha_{i'}$ for any $i'\in[n]$ then $\mathcal{A}$ aborts. If not, $\mathcal{A}$ respon s with $\mathbf{b}=\mathbf{f}(\boldsymbol{\beta})$ receiving right response $\tilde{\mathbf{b}}$.
- $\mathcal{A}$ checks whether $\tilde{b}_i=\tilde{a}_i$. If so, $\mathcal{A}$ outputs u', if not $\mathcal{A}$ outputs $1-u'$.

Just as in the proof of Claim 8, it suffices (by Fact 1) to construct an event $\mathbf{E}$ such that:

1. $\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbf{E}\big) \geq \frac{\varepsilon'\delta' p}{16}$;

2. $\Pr\big(\tilde{b}_i = \tilde{a}_i \big| u' = u \ \&\ \mathbf{E}\big) \geq \frac{\varepsilon'\delta\delta' p^3}{16}$;

3. $\Pr\big(\tilde{b}_i = \tilde{a}_i \big| u' \neq u \ \&\ \mathbf{E}\big) \leq \frac{\varepsilon^*}{n\varepsilon'\delta p^2}$,

since $\varepsilon^* \leq n\varepsilon'(\varepsilon'\delta\delta' p^3)^2/2048$. Temporarily let $Z = \big\{\tilde{\alpha}_i \in \big[2^{\tilde{t}_i}\big] : \big|\mathsf{HON}^i(\tilde{\alpha}_i)\big| \leq \tau\big|R^i(\tilde{\alpha}_i)\big|\big\}$, where i is the in ex chosen by $\mathcal{A}$ an $\tau = \varepsilon'\delta\delta' p^3/16$. Define the event

$$\mathbf{E} : \text{“}\mathbb{T} \in \mathsf{TRB} \cap \mathsf{IND} \setminus \mathsf{FIXED}\ \&\ \mathcal{A} \text{ oes not abort } \&\ \tilde{\alpha}_i \notin Z.\text{”}$$

Note that

$$\begin{aligned}
\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbf{E}\big) &\geq \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{IND} \setminus \mathsf{FIXED}\ \&\ \mathcal{A} \text{ not abort}\big) - \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\tilde{\alpha} \in Z\big) \\
&\geq -\frac{\varepsilon'\delta' p}{16} + \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{IND} \setminus \mathsf{FIXED}\big) \cdot \\
&\cdot \quad \Pr_{\tilde{\boldsymbol{\alpha}}\in\mathsf{HON}}\big(\mathcal{A} \text{ not abort}\big|\mathbb{T} \in \mathsf{TRB} \cap \mathsf{IND} \setminus \mathsf{FIXED}\big) \\
&\geq \frac{\delta' p}{8} \cdot \frac{1}{n} \cdot \varepsilon' n - \frac{\varepsilon'\delta' p}{16} = \frac{\varepsilon'\delta' p}{16},
\end{aligned}$$

by efinition of IND (the $1/n$ appears because $\mathcal{A}$ must guess the right value of $i \in [n]$). Moreover, as $\tilde{\alpha}_i \notin Z$, if $u' = u$ then M answers $\tilde{\boldsymbol{\beta}}$ an correctly on the right with probability at least $\varepsilon'\delta\delta' p^3/16$, which means that the probability that $\tilde{b}_i = \tilde{a}_i$ given $u' = u$ & $\mathbf{E}$ is at least as high.

Finally, we boun $\Pr\big(\tilde{b}_i = \tilde{a}_i \big| u' \neq u \ \&\ \mathbf{E}\big)$. It oes not quite work to try to use Claim 2 irectly to argue that M oes not answer $\tilde{\beta}_i$ correctly if $u' \neq u$. This is because the answers M receives if $u' \neq u$ are ran omly istribute (this is ensure by $\mathcal{A}$ aborting in case $\beta_{i'} = \alpha_{i'}$ for any i'), whereas the answers M receives to $\boldsymbol{\beta}$ from E are ran om only in the case that $\boldsymbol{\beta}$ iffers in every coor inate from the $\boldsymbol{\alpha}$ aske in the main threa . For this reason, we must also use the fact that $\mathbb{T} \notin \mathsf{FIXED}$.

Consi er now the interaction between M an E where the main threa E receives as input has **Com** as the commitment message but has unspecifie query an response messages. By efinition, if $\mathbf{Com} \notin \mathsf{FIXED}^{i'}$ for all i' (ensuring that the main threa E receives is not in FIXED), then for any $\gamma_{i'} \in \big[2^{t_{i'}}\big]$, $\Pr_{\tilde{\boldsymbol{\beta}}\in\mathsf{HON}}\big(\beta_{i'} = \gamma_{i'}\big) \leq \varepsilon$. It follows by the union boun that no matter what main threa left query $\boldsymbol{\gamma}$ occurs (we use $\boldsymbol{\gamma}$ so as not to be confuse with the $\boldsymbol{\alpha}$ that was aske by M uring its interaction with $\mathcal{A}$ above),

$$\Pr_{\tilde{\boldsymbol{\beta}}}\big(\beta_{i'} \neq \gamma_{i'} \ \forall\ i'\big) \geq (1 - n\varepsilon) \cdot \Pr_{\tilde{\boldsymbol{\beta}}}\big(\tilde{\boldsymbol{\beta}} \in \mathsf{HON}\big) \geq n\varepsilon'\delta p^2$$

(assuming also that **Com** is such that the transcript is in USEFUL). So we see that if the transcript E receives as input is in $\mathsf{TRB} \setminus \mathsf{FIXED}$, then a goo portion of the left queries which M asks uring its interaction with E will not share any coor inate with the main threa query, an so M will be given truly ran om responses. If in a ition, the transcript given to E is not in EXT then

$$\begin{aligned}
\varepsilon^* &\geq \Pr_{\tilde{\boldsymbol{\beta}}}\big(\text{M answers } \tilde{\beta}_i \text{ correctly}\big|\text{E answers } \boldsymbol{\beta}\big) \\
&\geq \Pr_{\tilde{\boldsymbol{\beta}}}\big(\text{M answers } \tilde{\beta}_i \text{ correctly}\big|\text{E answers } \boldsymbol{\beta} \ \&\ \beta_{i'} \neq \gamma_{i'} \ \forall\ i'\big) \cdot \Pr_{\tilde{\boldsymbol{\beta}}}\big(\beta_{i'} \neq \gamma_{i'} \ \forall\ i'\big) \\
&\geq \big(n\varepsilon'\delta p^2\big) \cdot \Pr_{\tilde{\boldsymbol{\beta}}}\big(\text{M answers } \tilde{\beta}_i \text{ correctly}\big|\boldsymbol{\beta} \text{ answere ran omly}\big).
\end{aligned}$$

An so we have

$$\begin{aligned}\Pr\big(\tilde{b}_i = \tilde{a}_i \big| u' \neq u \;\&\; \mathbf{E}\big) &= \Pr\big(\text{M answers } \tilde{\beta}_i \text{ corr.} \big| \boldsymbol{\beta} \text{ answere ran . } \& \; \mathbb{T} \in \mathsf{TRB} \setminus \mathsf{FIXED}\big) \\ &\leq \frac{\varepsilon^*}{n\varepsilon'\delta p^2},\end{aligned}$$

completing the proof of Claim 9. □

Claims 5 through 9 combine to give that if Com is computationally hi ing, then

$$\begin{aligned}\Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB}\big) &\leq \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{UNBAL}\big) + \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap 1{-}2\big) \\ &+ \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \cap \mathsf{IND}\big) + \Pr_{\mathbb{T}\in\mathsf{ACC}}\big(\mathbb{T} \in \mathsf{TRB} \setminus (\mathsf{UNBAL} \cup 1{-}2 \cup \mathsf{IND})\big) \\ &\leq \frac{\delta' p}{4} + \frac{\delta' p}{4} + \frac{\delta' p}{4} + \frac{\delta' p}{4} = \delta' p,\end{aligned}$$

completing the proof of Lemma 1, Theorem 2 an Theorem 1.

6 Non-Malleability in 4-Rounds

In this section we show how to squeeze our non-malleable protocol $\langle \mathrm{C}, \mathrm{R} \rangle$ into 4 roun s. In the new protocol, the zero-knowle ge messages are lifte up an sent together with the commit, challenge an response messages. We use a variant of the zero-knowle ge argument of knowle ge protocol of Feige an Shamir [FS90] in which V sets a trap oor by proving a har statement using a 3-roun witness-hi ing argument of knowle ge ($\mathcal{WHAOK}$) an P uses a 3-roun witness-in istinguishable argument of knowle ge ($\mathcal{WIAOK}$) to prove either the original statement $x \in L$ or knowle ge of V's trap oor. If we instantiate the $\mathcal{WIAOK}$ with the 3-roun $\mathcal{WIAOK}$ protocol of [FLS99] (where the statement to be proven can be chosen in the last roun), then the protocol can be parallelize own to four roun s. We comment that there exist protocols for proving knowle ge of commitment which are amenable to the Feige-Shamir parallelization technique without requiring a general $\mathcal{NP}-$re uction (such as Schnorr protocols base on DDH). Such protocols make a much better choice in practice.

We carefully parallelize the Feige-Shamir protocol with our 4-roun basic component of $\langle \mathrm{C}, \mathrm{R} \rangle$ an obtain the first 4-roun non-malleable commitment scheme. Our 4-roun commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$ appears in Figure 4. We slightly alter the $\mathcal{WHAOK}$ use in the original Feige-Shamir construction (which assumes the existence of OWPs) in or er to only rely on the existence of a OWF f. In the first roun , R chooses $2n$ ran om pairs (x_i^b, y_i^b) for $i = 1, \ldots, n$ an $b \in \{0,1\}$ such that $y_i^b = f(x_i^b)$, an sen s the y_i^b to C. Then C sen s a ran om challenge $z \in \{0,1\}^n$ an R returns $x_i^{z_i}$ for all i. C checks that in ee $y_i^{z_i} = f(x_i^{z_i})$ for all i (aborting if not) an uses a $\mathcal{WIAOK}$ to prove either the original statement, or knowle ge of some pair (x^0, x^1) such that $(y_i^0, y_i^1) = \big(f(x^0), f(x^1)\big)$ for some i. It can be checke that the resulting $4-$roun protocol is still ZK. We let π enote the $3-$roun $\mathcal{WIAOK}$.

Proposition 2. *If OWFs exist then* $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$ *is a* $4-$*round statistically binding, non-malleable commitment scheme.*

Proof Sketch. Statistical bin ing follows imme iately from the statistical bin ing property of Com. Computational hi ing is shown similarly to Proposition 1.

P blic Parameters: Tags $t_1, \dots, t_n$, prime q such that $q > 2^{t_i}$ for all i, an OWF $f : X \to Y$.

Commiter's Pri ate Inp t: Message $m \in \mathbb{F}_q$ to be committe to.

1. $\mathrm{R} \to \mathrm{C}$: Sample ran om $x_i^0, x_i^1 \in X$ for $i = 1, \dots, n$ an sen $(y_i^0, y_i^1)_i = \big(f(x_i^0), f(x_i^1)\big)_i$. Also sen σ, the first message of Naor's commitment scheme.

2. $\mathrm{C} \to \mathrm{R}$: Sen challenge $z \in \{0,1\}^n$ along with the first message of π an the commitment vector $\mathbf{Com} = \big(\mathrm{Com}_\sigma(m; s), \mathrm{Com}_\sigma(r_1; s_1), \dots, \mathrm{Com}_\sigma(r_n; s_n)\big)$ as one in Step 1 of $\langle \mathrm{C}, \mathrm{R} \rangle$. The statement of π will be etermine in step 4.

3. $\mathrm{R} \to \mathrm{C}$: Sen $x_i^{z_i}$ for $i = 1, \dots, n$ along with challenge message of π an the challenge vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ as one in Step 2 of $\langle \mathrm{C}, \mathrm{R} \rangle$.

4. $\mathrm{C} \to \mathrm{R}$: Sen the evaluation vector $\mathbf{a}$ where $a_i = r_i\alpha_i + m$ as in Step 3 of $\langle \mathrm{C}, \mathrm{R} \rangle$ along with the last message of π proving the statement:

   - EITHER: $\exists \, \big((m; s), (r_1; s_1), \dots, (r_n; s_n)\big)$ such that:
     - $\mathbf{Com} = \big(\mathrm{Com}_\sigma(m; s), \mathrm{Com}_\sigma(r_1; s_1), \dots, \mathrm{Com}_\sigma(r_n; s_n)\big)$; an
     - $a_i = r_i\alpha_i + m$ for all i;
   - OR: $\exists \, (x^0, x^1)$ such that $(y_i^0, y_i^1) = \big(f(x^0), f(x^1)\big)$ for some i.

Figure 4: : 4-roun non-malleable commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$.

The proof that $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$ is non-malleable against a synchronizing a versary follows exactly the same argument as the proof that $\langle \mathrm{C}, \mathrm{R} \rangle$ is non-malleable except that now when E is rewin ing an answering M's queries ran omly in the left interaction, it must complete π using M's trap oor statement. This is not a problem; it just means that before E can start rewin ing M back to the beginning of the right execution's query phase an trying to extract $\tilde{m}$, it must first rewin M back to the left execution's commit phase an extract M's trap oor witness.

In or er to prove non-malleability against a non-synchronizing M, we simply enumerate all of the other possibilities for M's sche uling an check that in all of them $\tilde{m}$ can be extracte . As $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$ has only four roun s, this is a very manageable task. It is easy to see that extraction is trivial from an M who uses any sche uling other than the synchronizing one. The key observations are: 1) an M who mauls must play the secon message on the left before the secon message on the right, 2) if the thir an fourth messages on the right are consecutive then E can extract $\tilde{m}$ from π. $\square$

Using our new commitment scheme $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$, we obtain a simple 4-roun non-malleable zero knowle ge argument $\langle \mathrm{P}, \mathrm{V} \rangle$ for any language $L \in \mathcal{NP}$. A etaile escription of $\langle \mathrm{P}, \mathrm{V} \rangle$ appears in Figure 5.

Proposition 3. *If OWFs exist then* $\langle \mathrm{P}, \mathrm{V} \rangle$ *is a* $4-$*round non-malleable zero knowledge argument of knowledge for any* $L \in \mathcal{NP}$.

Proof Sketch. The proof of non-malleability is similar to the non-malleability of $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$. The

P blic Inp t: Tags $t_1, \ldots, t_n$ in error correcte form, large prime q an OWF $f : X \to Y$.

Common inp t: $x \in L$.

Inp t to the pro er: A witness w for $x \in L$.

1. V $\to$ P: Sample ran om $x_i^b \in X$ for $i = 1, \ldots, n$ an $b \in \{0, 1\}$. Sen $y_i^b = f(x_i^b)$ along with the first message of $\langle \mathrm{C}(w), \mathrm{R} \rangle$.
2. P $\to$ V: Sen challenge $z \in \{0, 1\}^n$ along with the secon message of $\langle \mathrm{C}(w), \mathrm{R} \rangle$ an the first message of π for a statement to be proven later.
3. V $\to$ P: Sen $x_i^{z_i}$ for $i = 1, \ldots, n$, the thir message of $\langle \mathrm{C}(w), \mathrm{R} \rangle$ an the challenge message of π.
4. P $\to$ V: Sen the last message of $\langle \mathrm{C}(w), \mathrm{R} \rangle$ an the last message of π proving:
   - $x \in L$ an $\langle \mathrm{C}(w), \mathrm{R} \rangle$ was execute correctly; OR
   - $\exists\ (x^0, x^1)$ such that $(y_i^0, y_i^1) = \big(f(x^0), f(x^1)\big)$ for some i.

Figure 5: The 4-roun non malleable zero-knowle ge argument of knowle ge protocol $\langle \mathrm{P}, \mathrm{V} \rangle$.

zero-knowle ge property follows by the ZK of [FS90] an the hi ing of $\langle \mathrm{C}, \mathrm{R} \rangle_{\mathsf{OPT}}$. Lastly, the AOK property can be erive by constructing an extractor that behaves as a honest verifier an extracts the witness by rewin ing an sen ing ifferent challenges. $\square$

Towards 3-ro nd non-malleability. One natural question, in light of the above protocols, is "might we hope to obtain a 3−roun NMC scheme assuming OWPs exist" (say by replacing Naor's 2-roun bit commitment scheme with Blum's non-interactive one). However, this is unlikely as we nee four roun s for the ZK argument which runs alongsi e the commit, query, response messages. Moreover, attempts to replace the ZK argument with some sort of 3-roun WI run into the issue that E must extract M's trap oor on the secon roun . So it seems that significantly new i eas are require in or er to obtain 3-roun NMC. In light of the 3-roun lower boun of [Pas13] (using blackbox security re uctions), 3-roun NMC remains a fascinating open problem.

Acknowledgements

We woul like to thank the anonymous FOCS referees for very helpful comments an suggestions to earlier versions of this paper.

References

[Bar02] Boaz Barak. Constant-Roun Coin-Tossing with a Man in the Mi le or Realizing the Share Ran om String Mo el. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, FOCS '02, pages 345–355, 2002.

[CGMO09] Nishanth Chan ran, Vipul Goyal, Ryan Moriarty, an Rafail Ostrovsky. Position base cryptography. In Shai Halevi, e itor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 391–407. Springer, 2009.

[CLOS02] Ran Canetti, Yehu a Lin ell, Rafail Ostrovsky, an Amit Sahai. Universally composable two-party an multi-party secure computation. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, STOC '02, pages 494–503, 2002.

[DDN91] Danny Dolev, Cynthia Dwork, an Moni Naor. Non-Malleable Cryptography (Exten e Abstract). In *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*, STOC '91, pages 542–552, 1991.

[FLS99] Uriel Feige, Dror Lapi ot, an A i Shamir. Multiple non-interactive zero-knowle ge proofs un er general assumptions. *J. Comput. Syst. Sci.*, 29, 1999.

[FS90] Uriel Feige an A i Shamir. Witness in istinguishable an witness hi ing protocols. In *STOC*, pages 416–426. ACM, 1990.

[GLOV12] Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, an Ivan Visconti. Constructing non-malleable commitments: A black-box approach. In *FOCS*, pages 51–60. IEEE Computer Society, 2012.

[Goy11] Vipul Goyal. Constant Roun Non-malleable Protocols Using One-way Functions. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, STOC '11, pages 695–704. ACM, 2011.

[HILL99] Johan Håsta , Russell Impagliazzo, Leoni A. Levin, an Michael Luby. A Pseu o-ran om Generator from any One-way Function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, an Amit Sahai. Zero-knowle ge from Secure Multiparty Computation. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, STOC '07, pages 21–30, 2007.

[KOS03] Jonathan Katz, Rafail Ostrovsky, an A am Smith. Roun Efficiency of Multi-party Computation with a Dishonest Majority. In *Advances in Cryptology — EUROCRYPT ' 3*, volume 2656 of *Lecture Notes in Computer Science*, pages 578–595. Springer, 2003.

[LP11] Huijia Lin an Rafael Pass. Constant-roun Non-malleable Commitments from Any One-way Function. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, STOC '11, pages 705–714, 2011.

[LPV08] Huijia Lin, Rafael Pass, an Muthuramakrishnan Venkitasubramaniam. Concurrent Non-malleable Commitments from Any One-Way Function. In *Theory of Cryptography, 5th Theory of Cryptography Conference, TCC 8*, pages 571–588, 2008.

[LPV09] Huijia Lin, Rafael Pass, an Muthuramakrishnan Venkitasubramaniam. A Unifie Framework for Concurrent Security: Universal Composability from Stan -alone Non-malleability. In *Proceedings of the 4 st Annual ACM Symposium on Theory of Computing*, STOC '09, pages 179–188, 2009.

[Nao91] Moni Naor. Bit Commitment Using Pseu oran omness. *J. Cryptology*, 4(2):151–158, 1991.

[NSS06] Moni Naor, Gil Segev, an A am Smith. Tight boun s for uncon itional authentication protocols in the manual channel an share key mo els. In Cynthia Dwork, e itor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 214–231. Springer, 2006.

[Pas04] Rafael Pass. Boun e -Concurrent Secure Multi-Party Computation with a Dishonest Majority. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, STOC '04, pages 232–241, 2004.

[Pas13] Rafael Pass. Unprovable security of perfect nizk an non-interactive non-malleable commitments. pages 334–354, 2013.

[PR05] Rafael Pass an Alon Rosen. New an improve constructions of non-malleable cryptographic protocols. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, STOC '05, pages 533–542, 2005.

[PW10] Rafael Pass an Hoeteck Wee. Constant-Roun Non-malleable Commitments from Sub-exponential One-Way Functions. In *Advances in Cryptology — EUROCRYPT '* , pages 638–655, 2010.

[Sha79] A i Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, 1979.

[Wee10] Hoeteck Wee. Black-Box, Roun -Efficient Secure Computation via Non-malleability Amplification. In *Proceedings of the 5 th Annual IEEE Symposium on Foundations of Computer Science*, pages 531–540, 2010.