Coin Flipping of *Any* Constant Bias Implies One-Way Functions

ITAY BERMAN, Massachusetts Institute of Technology
IFTACH HAITNER, Tel Aviv University
ARIS TENTES

We show that the existence of a coin-flipping protocol safe against *any* nontrivial constant bias (e.g., .499) implies the existence of one-way functions. This improves upon a result of Haitner and Omri (FOCS'11), who proved this implication for protocols with bias $\frac{\sqrt{2}-1}{2} - o(1) \approx .207$. Unlike the result of Haitner and Omri, our result also holds for *weak* coin-flipping protocols.

CCS Concepts: • **Security and privacy** → **Mathematical foundations of cryptography**; • **Theory of computation** → **Cryptographic primitives**;

Additional Key Words and Phrases: Coin-flipping protocols, one-way functions, minimal hardness assumptions

ACM Reference format:
Itay Berman, Iftach Haitner, and Aris Tentes. 2018. Coin Flipping of *Any* Constant Bias Implies One-Way Functions. *J. ACM* 65, 3, Article 14 (March 2018), 95 pages.
https://doi.org/10.1145/2979676

1 INTRODUCTION

A central focus of modern cryptography has been to investigate the weakest possible assumptions under which various cryptographic primitives exist. This direction of research has been quite fruitful, and minimal assumptions are known for a wide variety of primitives. In particular, it has been shown that one-way functions (i.e., easy to compute but hard to invert) imply pseudorandom generators, pseudorandom functions, symmetric-key encryption/message authentication,

An extended abstract of this work appeared in the Proceedings of STOC 2014 [3].
Most of this work was done while I. Berman was in the School of Computer Science, Tel Aviv University.
Most of this work was done while A. Tentes was in the Department of Computer Science, New York University.

The work is supported by Israel Science Foundation (ISF) under Grant No.: 1076/11 G1, the Israeli Centers of Research Excellence (I-CORE) program under Center No.: 4/11 (http://www.icore-algo.org.il/), the United states – Israel Binational Science Foundation under Grant No.: 2010196 and Check Point Institute for Information Security.
The first author is also supported in part by the National Science Foundation (NSF) under Grants No.: CNS-1413920 and CNS-1350619, and by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts No.: W911NF-15-C-0226 and W911NF-15-C-0236.

Authors' addresses: I. Berman, Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory (CSAIL), office 32G-578, 32 Vassar St, Cambridge, MA, 02139; email: itayberm@mit.edu; I. Haitner, Tel Aviv University, School of Computer Science, P.O.B. 39040, Ramat Aviv, Tel Aviv, 69978, Israel; email: iftachh@cs.tau.ac.il; A. Tentes; email: tentes@cims.nyu.edu.

https://doi.org/10.1145/2979676

commitment schemes, and digital signatures [9–12, 14, 21, 22, 24], where one-way functions were also shown to be implied by each of these primitives [16].

An important exception to the above successful characterization is that of coin-flipping (-tossing) protocols. A coin-flipping protocol [4] allows the honest parties to jointly flip an unbiased coin, where even a cheating (efficient) party cannot bias the outcome of the protocol by very much. Specifically, a coin-flipping protocol is δ-biased if no efficient cheating party can make the common output to be 1, or to be 0, with probability greater than $\frac{1}{2} + \delta$. While one-way functions are known to imply negligible-bias coin-flipping protocols [4, 14, 21], the other direction is less clear. Impagliazzo and Luby [16] showed that $\Theta(1/\sqrt{m})$-bias coin-flipping protocols imply one-way functions, where m is the number of rounds in the protocol.[1] Recently, Maji et al. [18] extended the above for $(\frac{1}{2} - 1/\operatorname{poly}(n))$-bias *constant-round* protocols, where n is the security parameter. More recently, Haitner and Omri [13] showed that the above implication holds for $(\frac{\sqrt{2}-1}{2} - o(1) \approx 0.207)$-bias coin-flipping protocols (of arbitrary round complexity). No such implications were known for any other choice of parameters, and in particular for protocols with bias greater than $\frac{\sqrt{2}-1}{2}$ with super-constant round complexity.

1.1 Our Result

In this work, we make progress toward answering the question of whether coin-flipping protocols also imply one-way functions. We show that (even weak) coin-flipping protocols, safe against any nontrivial bias (e.g., 0.4999), do in fact imply such functions. We note that unlike [13], but like [16, 18], our result also applies to the so-called *weak coin-flipping protocols* (see Section 2.3 for the formal definition of strong and weak coin-flipping protocols). Specifically, we prove the following theorem.

Theorem 1.1 (Informal). *For any $c > 0$, the existence of a $(\frac{1}{2} - c)$-bias coin-flipping protocol (of any round complexity) implies the existence of one-way functions.*

Note that the $\frac{1}{2}$-bias coin-flipping protocol requires no assumption (i.e., one party flips a coin and announces the result to the other party). So our result is tight as long as constant biases (i.e., independent of the security parameter) are involved.

To prove Theorem 1.1, we observe a connection between the success probability of the best (valid) attacks in a two-party game (e.g., tic-tac-toe) and the success of the biased-continuation attack of [13] in winning this game (see more in Section 1.3). The implications of this interesting connection seem to extend beyond the question at the focus of this article.

1.2 Related Results

As mentioned above, Impagliazzo and Luby [16] showed that negligible-bias coin-flipping protocols imply one-way functions. Maji et al. [18] proved the same for $(\frac{1}{2} - o(1))$-bias yet constant-round protocols. Finally, Haitner and Omri [13] showed that the above implication holds for $\frac{\sqrt{2}-1}{2} - o(1) \approx 0.207)$-bias (strong) coin-flipping protocols (of arbitrary round complexity). Results of weaker complexity implications are also known.

Zachos [25] has shown that nontrivial (i.e., $(\frac{1}{2} - o(1))$-bias) constant-round coin-flipping protocols imply that NP $\not\subseteq$ BPP, where Maji et al. [18] proved the same implication for $(\frac{1}{4} - o(1))$-bias coin-flipping protocols of arbitrary round complexity. Finally, it is well known that the existence of nontrivial coin-flipping protocols implies that PSPACE $\not\subseteq$ BPP. Apart from [13], all the above results extend to weak coin-flipping protocols. See Table 1 for a summary.

[1] In [16], only $\operatorname{neg}(m)$-bias was stated. Proving the same implication for $\Theta(1/\sqrt{m})$-bias follows from the proof outlined in [16] and the result by Cleve and Impagliazzo [7].

Table 1. Results Summary

Implication	*Protocol Type*	*Article*
Existence of OWFs	$(\frac{1}{2} - c)$-bias, for some $c > 0$	**This work**
Existence of OWFs	$(\frac{\sqrt{2}-1}{2} - o(1))$-bias	Haitner and Omri [13][2]
Existence of OWFs	$(\frac{1}{2} - o(1))$-bias, *constant round*	Maji et al. [18]
Existence of OWFs	Negligible bias	Impagliazzo and Luby [16]
$\mathrm{NP} \not\subseteq \mathrm{BPP}$	$(\frac{1}{4} - o(1))$-bias	Maji et al. [18]
$\mathrm{NP} \not\subseteq \mathrm{BPP}$	$(\frac{1}{2} - o(1))$-bias, *constant round*	Zachos [25]
$\mathrm{PSPACE} \not\subseteq \mathrm{BPP}$	Nontrivial	Common knowledge

Information theoretic coin-flipping protocols (i.e., whose security holds against all-powerful attackers) were shown to exist in the quantum world; Mochon [19] presented an ε-bias quantum weak coin-flipping protocol for any $\varepsilon > 0$. Chailloux and Kerenidis [5] presented a $(\frac{\sqrt{2}-1}{2} - \varepsilon)$-bias quantum strong coin-flipping protocol for any $\varepsilon > 0$ (this bias was shown in [17] to be tight). A key step in [5] is a reduction from strong to weak coin-flipping protocols, which holds also in the classical world.

A related line of work considers *fair* coin-flipping protocols. In this setting, the honest party is required to always output a bit, whatever the other party does. In particular, a cheating party might bias the output coin just by aborting. We know that one-way functions imply fair $(1/\sqrt{m})$-bias coin-flipping protocols [1, 6], where m is the round complexity of the protocol, and this quantity is known to be tight for $o(m/\log m)$-round protocols with fully black-box reductions [8]. Oblivious transfer, on the other hand, implies fair $1/m$-bias protocols [2, 20] (this bias was shown in [6] to be tight).

1.3 Our Techniques

The following is a rather elaborate, high-level description of the ideas underlying our proof.

That the existence of a given (cryptographic) primitive implies the existence of one-way functions is typically proven by looking at the *primitive core function*—an efficiently computable function (not necessarily unique) whose inversion on uniformly chosen outputs implies breaking the security of the primitive.[3] For private-key encryption, for instance, a possible core function is the mapping from the inputs of the encryption algorithm (i.e., message, secret key, and randomness) into the ciphertexts. Assuming that one has defined such a core function for a given primitive, then, by definition, this function should be one-way. So it all boils down to finding, or proving the existence of, such a core function for the primitive under consideration. For a *noninteractive* primitive, finding such a core function is typically easy. In contrast, for an *interactive* primitive, finding such a core function is, at least in many settings, a much more involved task. The reason is that in order to break an interactive primitive, the attacker typically needs, for a given function, preimages for many different outputs, where these outputs are chosen *adaptively* by the attacker, after seeing the preimages to the previous outputs. As a result, it is challenging to find a single function, or even finitely many functions, whose output distributions (on uniformly chosen input) match the distribution of the preimages the attacker needs.[4]

[2] Only holds for *strong* coin-flipping protocols.

[3] For the sake of this informal discussion, inverting a function on a given value means returning a *uniformly* chosen preimage of this value.

[4] If the attacker makes a *constant* number of queries, one can overcome the above difficulty by defining a set of core functions $f_1, \ldots, f_k$, where f_1 is the function defined by the primitive, f_2 is the function defined by the attacker after making the

The only plausible candidate to serve as a core function of a coin-flipping protocol would seem to be its *transcript function*: the function that maps the parties' randomness into the resulting protocol transcript (i.e., the transcript produced by executing the protocol with this randomness). In order to bias the output of an m-round coin-flipping protocol by more than $O(\frac{1}{\sqrt{m}})$, a super-constant number of adaptive inversions of the transcript function seems necessary. Yet we managed to prove that the transcript function is a core function of any (constant-bias) coin-flipping protocol. This is done by designing an adaptive attacker for any such protocol whose query distribution is "not too far" from the output distribution of the transcript function (when invoked on uniform inputs). Since our attacker, described below, is not only adaptive but also defined in a recursive manner, proving that it possesses the aforementioned property was one of the major challenges we faced.

In what follows, we give a high-level overview of our attacker that ignores computational issues (i.e., assumes it has a perfect inverter for any function). We then explain how to adjust this attacker to work with the inverter of the protocol's transcript function.

1.3.1 Optimal Valid Attacks and the Biased-Continuation Attack. The crux of our approach lies in an interesting connection between the optimal attack on a coin-flipping protocol and the more feasible, *recursive biased-continuation* attack. The latter attack recursively applies the biased-continuation attack used by Haitner and Omri [13] to achieve their constant-bias attack (called there the *random-continuation* attack) and is the basis of our efficient attack (assuming one-way functions do not exist) on coin-flipping protocols. The results outlining the aforementioned connection, informally stated in this section and formally stated and proven in Section 3, hold for any two-player full information game with binary common outcome.

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a coin-flipping protocol (i.e., the common output of the honest parties is a uniformly chosen bit). In this discussion, we restrict ourselves to analyzing attacks that, when carried out by the left-hand party, i.e., A, are used to bias the outcome toward one, and when carried out by the right-hand party, i.e., B, are used to bias the outcome toward zero. Analogous statements hold for opposite attacks (i.e., attacks carried out by A and used to bias toward zero, and attacks carried out by B and used to bias toward one). The optimal valid attacker $\mathcal{A}$ carries out the *best* attack A can employ (using unbounded power) to bias the protocol toward *one*, while sending *valid* messages—ones that could have been sent by the honest party. The optimal valid attacker $\mathcal{B}$, carrying out the best attack B can employ to bias the protocol toward *zero*, is analogously defined. Since, without loss of generality, the optimal valid attackers are deterministic, the expected outcome of $(\mathcal{A}, \mathcal{B})$ is either zero or one. As a first step, we give a lower bound on the success probability of the recursive biased-continuation attack carried out by the party winning the aforementioned game. As this lower bound might not be sufficient for our goal (it might be less than constant)—and this is a crucial point in the description below—our analysis takes additional steps to give an arbitrarily-close-to-one lower bound on the success probability of the recursive biased-continuation attack carried out by *some* party, which may or may not be the same party winning the aforementioned game.[5]

Assume that $\mathcal{A}$ is the winning party when playing against $\mathcal{B}$. Since $\mathcal{A}$ sends only valid messages, it follows that the expected outcome of $(\mathsf{A}, \mathcal{B})$, i.e., honest A against the optimal attacker for B,

first inversion call, and so on. Since the evaluation time of f_{i+1} is polynomial in the evaluation time of f_i (since evaluating f_{i+1} requires a call to an inverter of f_i), this approach fails miserably for attackers of super-constant query complexity.

[5] That the identity of the winner in $(\mathcal{A}, \mathcal{B})$ cannot be determined by the recursive biased-continuation attack is crucial. Since we show that the latter attack can be efficiently approximated assuming one-way functions do not exist, the consequences of revealing this identity would be profound. It would mean that we can estimate the outcome of the optimal attack (which is implemented in PSPACE) using only the assumption that one-way functions do not exist.

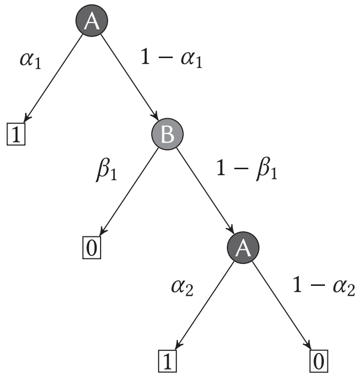


Fig. 1. Coin-flipping protocol Π. The label of an internal node (i.e., partial transcript) denotes the name of the party controlling it (i.e., the party that sends the next message given this partial transcript), and that of a leaf (i.e., full transcript) denotes its value—the parties' common output once reaching this leaf. Finally, the label on an edge leaving a node u to node u' denotes the probability that a random execution of Π visits u' once in u.
Note that $\mathrm{OPT}_{\mathrm{A}}(\Pi) = 1$ and $\mathrm{OPT}_{\mathrm{B}}(\Pi) = 1 - \alpha_1$. The A-dominated set $\mathcal{S}^{\mathrm{A}}$ in this case consists of the single 1-leaf to the left of the root. The conditional protocol Π' is the protocol rooted in the node to the right of the root (of Π), and the B$'$-dominated set $\mathcal{S}^{\mathrm{B}}$ consists of the single 0-leaf to the left of the root of Π'.

is larger than zero (since A might send the optimal messages "by mistake"). Let $\mathrm{OPT}_{\mathrm{A}}(\Pi)$ be the expected outcome of the protocol $(\mathcal{A}, \mathrm{B})$ and let $\mathrm{OPT}_{\mathrm{B}}(\Pi)$ be 1 minus the expected outcome of the protocol $(\mathrm{A}, \mathcal{B})$. The above observation yields that $\mathrm{OPT}_{\mathrm{A}}(\Pi) = 1$, while $\mathrm{OPT}_{\mathrm{B}}(\Pi) = 1 - \alpha < 1$. This gives rise to the following question: *what does give $\mathcal{A}$ an advantage over $\mathcal{B}$?*

We show that if $\mathrm{OPT}_{\mathrm{B}}(\Pi) = 1 - \alpha$, then there exists a set $\mathcal{S}^{\mathrm{A}}$ of 1-transcripts, full transcripts in which the parties' common output is 1,[6] that is α-dense (meaning that the chance that a random full transcript of the protocol is in the set is α) and is "dominated by A." The A-dominated set has an important property—its density is "immune" to any action B might take, even if B is employing its optimal attack; specifically, the following holds:

$$\Pr_{\langle \mathrm{A}, \mathrm{B} \rangle}\left[\mathcal{S}^{\mathrm{A}}\right] = \Pr_{\langle \mathrm{A}, \mathcal{B} \rangle}\left[\mathcal{S}^{\mathrm{A}}\right] = \alpha, \tag{1}$$

where $\langle \Pi' \rangle$ samples a random full transcript of protocol Π'. It is easy to see that the above holds if A controls the root of the tree and has a 1-transcript as a direct descendant; see Figure 1 for a concrete example. The proof of the general case can be found in Section 3. Since the A-dominated set is B-immune, a possible attack for $\mathcal{A}$ is to go toward this set. Hence, what seems like a feasible adversarial attack for A is to mimic $\mathcal{A}$'s attack by hitting the A-dominated set with high probability. It turns out that the biased-continuation attack of [13] does exactly that.

The biased-continuation attacker $\mathrm{A}^{(1)}$, taking the role of A in Π and trying to bias the output of Π toward one, is defined as follows: given that the partial transcript is trans, algorithm $\mathrm{A}^{(1)}$ samples a pair of random coins $(r_{\mathrm{A}}, r_{\mathrm{B}})$ that is consistent with trans and leads to a 1-transcript, and then acts as the honest A on the random coins r_{A}, given the transcript trans. In other words, $\mathrm{A}^{(1)}$ takes the first step of a random continuation of (A, B) leading to a 1-transcript. (The attacker $\mathrm{B}^{(1)}$, taking the role of B and trying to bias the outcome toward zero, is analogously defined.) Haitner

[6] Throughout, we assume without loss of generality that the protocol's transcript determines the common output of the parties.

and Omri [13] showed that for any coin-flipping protocol, if either A or B carries out the biased-continuation attack toward one, the outcome of the protocol will be biased toward one by $\frac{\sqrt{2}-1}{2}$ (when interacting with the honest party).[7] Our basic attack employs the above biased-continuation attack recursively. Specifically, for $i > 1$, we consider the attacker $\mathsf{A}^{(i)}$ that takes the first step of a random continuation of $(\mathsf{A}^{(i-1)}, \mathsf{B})$ leading to a 1-transcript, letting $\mathsf{A}^{(0)} \equiv \mathsf{A}$. The attacker $\mathsf{B}^{(i)}$ is analogously defined. Our analysis takes a different route from that of [13], whose approach is only applicable for handling bias up to $\frac{\sqrt{2}-1}{2}$ and cannot be applied to weak coin-flipping protocols.[8] Instead, we analyze the probability of the biased-continuation attacker to hit the dominated set we introduced above.

Let trans be a 1-transcript of Π in which all messages are sent by A. Since $\mathsf{A}^{(1)}$ picks a random 1-transcript, and B cannot force $\mathsf{A}^{(1)}$ to diverge from this transcript, the probability to produce trans under an execution of $(\mathsf{A}^{(1)}, \mathsf{B})$ is *doubled* with respect to this probability under an execution of (A, B) (assuming the expected outcome of (A, B) is 1/2). The above property, that B cannot force $\mathsf{A}^{(1)}$ to diverge from a transcript, is in fact the B-immune property of the A-dominated set. A key step we take is to generalize the above argument to show that for the α-dense A-dominated set $\mathcal{S}^{\mathsf{A}}$ (which exists assuming that $\mathrm{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha < 1$), it holds that

$$\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] \geq \frac{\alpha}{\mathsf{val}(\Pi)}, \tag{2}$$

where $\mathsf{val}(\Pi')$ is the expected outcome of Π'. Namely, in $(\mathsf{A}^{(1)}, \mathsf{B})$, the probability of hitting the set $\mathcal{S}^{\mathsf{A}}$ of 1-transcripts is larger by a factor of at least $\frac{1}{\mathsf{val}(\Pi)}$ than the probability of hitting this set in the original protocol Π. Again, it is easy to see that the above holds if A controls the root of the tree and has a 1-transcript as a direct descendant; see Figure 1 for a concrete example. The proof of the general case can be found in Section 3.

Consider now the protocol $(\mathsf{A}^{(1)}, \mathsf{B})$. In this protocol, the probability of hitting the set $\mathcal{S}^{\mathsf{A}}$ is at least $\frac{\alpha}{\mathsf{val}(\Pi)}$, and clearly the set $\mathcal{S}^{\mathsf{A}}$ remains B-immune. Hence, we can apply Equation (2) again, to deduce that

$$\Pr_{\langle \mathsf{A}^{(2)}, \mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] = \Pr_{\langle (\mathsf{A}^{(1)})^{(1)}, \mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] \geq \frac{\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right]}{\mathsf{val}(\mathsf{A}^{(1)}, \mathsf{B})} \geq \frac{\alpha}{\mathsf{val}(\Pi) \cdot \mathsf{val}(\mathsf{A}^{(1)}, \mathsf{B})}. \tag{3}$$

Continuing it for κ iterations yields that

$$\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \geq \Pr_{\langle \mathsf{A}^{(\kappa)}, \mathsf{B} \rangle}\left[\mathcal{S}^{\mathsf{A}}\right] \geq \frac{\alpha}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}. \tag{4}$$

So, modulo some cheating,[9] it seems that we are in good shape. Taking, for example, $\kappa = \log(\frac{1}{\alpha})/\log(\frac{1}{0.9})$, Equation (4) yields that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) > 0.9$. Namely, if we assume that $\mathcal{A}$ has an advantage over $\mathcal{B}$, then by recursively applying the biased-continuation attack for A enough times,

[7] They show that the same holds for the analogous attackers carrying out the biased-continuation attack toward zero.

[8] A key step in the analysis of Haitner and Omri [13] is to consider the "all-cheating protocol" $(\mathsf{A}^{(1),1}, \mathsf{B}^{(1),1})$, where $\mathsf{A}^{(1),1}$ and $\mathsf{B}^{(1),1}$ take the roles of A and B, respectively, and they both carry out the biased-continuation attack trying to bias the outcome toward one (as opposed to having the attacker taking the role of B trying to bias the outcome toward zero, as in the discussion so far). Since, and this is easy to verify, the expected outcome of $(\mathsf{A}^{(1),1}, \mathsf{B}^{(1),1})$ is one, using symmetry, one can show that the expected outcome of either $(\mathsf{A}^{(1),1}, \mathsf{B})$ or $(\mathsf{A}, \mathsf{B}^{(1),1})$ is at least $\frac{1}{\sqrt{2}}$, yielding a bias of $\frac{1}{\sqrt{2}} - \frac{1}{2}$. As mentioned in [13], symmetry cannot be used to prove a bias larger than $\frac{1}{\sqrt{2}} - \frac{1}{2}$.

[9] The actual argument is somewhat more complicated than the one given above. To ensure that the above argument holds, we need to consider measures over the 1-transcripts (and not sets). In addition, while (the measure variant of) Equation (3) is correct, deriving it from Equation (2) takes some additional steps.

we arbitrarily bias the expected output of the protocol toward one. Unfortunately, if this advantage (i.e., $\alpha = (1 - \mathsf{OPT}_{\mathsf{B}}(\Pi))$) is very small, which is the case in typical examples, the number of recursions required might be linear in the protocol depth (or even larger). Given the recursive nature of the above attack, the running time of the described attacker is *exponential*. To overcome this obstacle, we consider not only the dominated set but also additional sets that are "close to" being dominated. Informally, we can say that a 1-transcript belongs to the A-dominated set if it can be generated by an execution of $(\mathcal{A}, \mathsf{B})$. In other words, the probability, over B's coins, that a transcript generated by a random execution of $(\mathcal{A}, \mathsf{B})$ belongs to the A-dominated set is one. We define a set of 1-transcripts that does not belong to the A-dominated set to be "close to" A-dominated if there is an (unbounded) attacker $\widehat{\mathcal{A}}$, such that the probability, over B's coins, that a transcript generated by a random execution of $(\widehat{\mathcal{A}}, \mathsf{B})$ belongs to the set is close to one. These sets are formally defined via the notion of conditional protocols, discussed next.

Conditional Protocols. Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a coin-flipping protocol in which there exists an A-dominated set $\mathcal{S}^{\mathsf{A}}$ of density $\alpha > 0$. Consider the "conditional" protocol $\Pi' = (\mathsf{A}', \mathsf{B}')$, resulting from conditioning on not hitting the set $\mathcal{S}_{\mathsf{A}}$. Namely, the message distribution of Π' is that induced by a random execution of Π that does not generate transcripts in $\mathcal{S}_{\mathsf{A}}$.[10] See Figure 1 for a concrete example. We note that the protocol Π' might not be efficiently computable (even if Π is), but this does not bother us, since we only use it as a thought experiment.

We have effectively removed all the 1-transcripts dominated by A (the set $\mathcal{S}^{\mathsf{A}}$ must contain all such transcripts; otherwise, $\mathsf{OPT}_{\mathsf{B}}(\Pi)$ would be smaller than $1 - \alpha$). Thus, the expected outcome of $(\mathcal{A}', \mathcal{B}')$ is zero, where $\mathcal{A}'$ and $\mathcal{B}'$ are the optimal valid attackers of the parties in the conditional protocol Π'. Therefore, $\mathsf{OPT}_{\mathsf{B}'}(\Pi') = 1$ and $\mathsf{OPT}_{\mathsf{A}'}(\Pi') = 1 - \beta < 1$. It follows from this crucial observation that there exists a B′-dominated $\mathcal{S}^{\mathsf{B}}$ of density β, over the 0-transcripts of Π'. Applying a similar argument to that used for Equation (4) yields that for large enough κ, the biased-continuation attacker $\mathsf{B}'^{(\kappa)}$, playing the role of B', succeeds in biasing the outcome of Π' toward zero, where κ is proportional to $\log(\frac{1}{\beta})$. Moreover, if α is small, the above yields that $\mathsf{B}^{(\kappa)}$ does almost equally well in the original protocol Π. If β is also small, we can now consider the conditional protocol Π'', obtained by conditioning Π' on not hitting the B′-dominated set, and so on.

By iterating the above process enough times, the A-dominated sets cover all the 1-transcripts, and the B-dominated sets cover all the 0-transcripts.[11] Assume that in the above iterated process, the density of the A-dominated sets is the first to go beyond $\varepsilon > 0$. It can be shown—and this a key technical contribution of this article—that it is almost as good as if the density of the *initial* set $\mathcal{S}_{\mathsf{A}}$ was ε.[12] We can now apply the above analysis and conclude that for any constant $\varepsilon > 0$, there exists a constant $\kappa = \kappa(\varepsilon)$ such that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) > 1 - \varepsilon$.[13]

[10] More formally, the conditional protocol Π' is defined as follows. Let trans be a partial transcript, and let p be the probability, in Π, that the message following trans is 0. Let α be the probability of generating a transcript in $\mathcal{S}^{\mathsf{A}}$ for which trans is a prefix and similarly let α_0 be the probability of generating a transcript in $\mathcal{S}^{\mathsf{A}}$ for which trans $\circ$ 0 is a prefix (trans $\circ$ 0 is the transcript trans followed by the message 0). Then, the probability that the message following trans is 0 in Π' is $p \cdot (1 - \alpha_0)/(1 - \alpha)$.

[11] When considering measures and not sets, as done in the actual proof, this covering property is not trivial.

[12] More accurately, let $\widetilde{\mathcal{S}}^{\mathsf{A}}$ be the union of these 1-transcript sets and let $\widetilde{\alpha}$ be the density of $\widetilde{\mathcal{S}}^{\mathsf{A}}$ in Π. Then $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \geq \Pr_{\langle \mathsf{A}^{(\kappa)}, \mathsf{B} \rangle}[\widetilde{\mathcal{S}}^{\mathsf{A}}] \geq \frac{\widetilde{\alpha}}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}$.

[13] The assumption that the density of the A-dominated sets is the first to go beyond $\varepsilon > 0$ is independent of the assumption that $\mathcal{A}$ wins in the zero-sum game $(\mathcal{A}, \mathcal{B})$. Specifically, the fact that $\mathsf{A}^{(\kappa)}$ succeeds in biasing the protocol does not guarantee that $\mathcal{A}$, which we only know how to implement in PSPACE, is the winner of $(\mathcal{A}, \mathcal{B})$.

1.3.2 Using the Transcript Inverter. We have seen above that for any constant ε, by recursively applying the biased-continuation attack for constantly many times, we get an attack that biases the outcome of the protocol by $\frac{1}{2} - \varepsilon$. The next thing is to implement the above attack *efficiently*, under the assumption that one-way functions do not exist. Given a partial transcript u of protocol Π, we wish to return a uniformly chosen full transcript of Π that is consistent with u and the common outcome it induces is one. Biased continuation can be reduced to the task of finding *honest continuation*: returning a uniformly chosen full transcript of Π that is consistent with u. Assuming honest continuation can be found for the protocol, biased-continuation can also be found by calling the honest continuation many times, until a transcript whose output is one is obtained. The latter can be done efficiently, as long as the value of the partial transcript u—the expected outcome of the protocol conditioned on u—is not too low. (If it is too low, too much time might pass before a full transcript leading to one is obtained.) Ignoring this low-value problem, and noting that honest continuation of a protocol can be reduced to inverting the protocol's transcript function, all we need to do to implement $\mathsf{A}^{(i)}$ is to invert the transcript functions of the protocols $(\mathsf{A}, \mathsf{B}), (\mathsf{A}^{(1)}, \mathsf{B}), \ldots, (\mathsf{A}^{(i-1)}, \mathsf{B})$. Furthermore, noting that the attackers $\mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(i-1)}$ are *stateless*, it suffices to have the ability to invert *only* the transcript function of (A, B).

So attacking a coin-flipping protocol Π boils down to inverting the transcript function f_Π of Π, and making sure we are not doing that on low-value transcripts. Assuming one-way functions do not exist, there exists an efficient inverter Inv for f_Π that is guaranteed to work well when invoked on random outputs of f_Π (i.e., when f_Π is invoked on the uniform distribution; nothing is guaranteed for distributions far from uniform). By the above discussion, algorithm Inv implies an efficient approximation of $\mathsf{A}^{(i)}$, as long as the partial transcripts attacked by $\mathsf{A}^{(i)}$ are neither *low value* nor *unbalanced* (by low-value transcript we mean that the expected outcome of the protocol conditioned on the transcript is low; by unbalanced transcript we mean that its density with respect to $(\mathsf{A}^{(i)}, \mathsf{B})$ is not too far from its density with respect to (A, B)). Whereas the authors of [13] proved that the queries of $\mathsf{A}^{(1)}$ obey the two conditions with sufficiently high probability, we were unable to prove this (and believe it is untrue) for the queries of $\mathsf{A}^{(i)}$, for $i > 1$. Thus, we simply cannot argue that $\mathsf{A}^{(i)}$ has an efficient approximation, assuming one-way functions do not exist. Fortunately, we managed to prove the above for the "pruned" variant of $\mathsf{A}^{(i)}$, defined below.

Unbalanced and low-value transcripts. Before defining our final attacker, we relate the problem of unbalanced transcripts to that of low-value transcripts. We say that a (partial) transcript u is *γ-unbalanced* if the probability that u is visited with respect to a random execution of $(\mathsf{A}^{(1)}, \mathsf{B})$ is at least γ times larger than with respect to a random execution of (A, B). Furthermore, we say that a (partial) transcript u is *δ-small* if the expected outcome of (A, B), conditioned on visiting u, is at most δ. We prove (a variant of) the following statement. For any $\delta > 0$ and $\gamma > 1$, there exists c that depends on δ, such that

$$\Pr_{\ell \leftarrow \langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}[\ell \text{ has a } \gamma\text{-unbalanced prefix but no } \delta\text{-small prefix}] \leq \frac{1}{\gamma^c}. \tag{5}$$

Namely, as long as $(\mathsf{A}^{(1)}, \mathsf{B})$ does not visit a low-value transcript, it is only at low risk to significantly deviate (in a multiplicative sense) from the distribution induced by (A, B). Equation (5) naturally extends to recursive biased-continuation attacks. It also has an equivalent form for the attacker $\mathsf{B}^{(1)}$, trying to bias the protocol toward zero, with respect to δ-high transcripts—the expected outcome of Π, conditioned on visiting the transcript, is at least $1 - \delta$.

The pruning attacker. At last we are ready to define our final attacker. To this end, for protocol $\Pi = (\mathsf{A}, \mathsf{B})$, we define its *$\delta$-pruned variant* $\Pi_\delta = (\mathsf{A}_\delta, \mathsf{B}_\delta)$, where $\delta \in (0, \frac{1}{2})$, as follows. As long as the execution does not visit a δ-low or δ-high transcript, the parties act as in Π. Once a δ-low transcript is visited, only the party B sends messages, and it does so according to the distribution induced by Π. If a δ-high transcript is visited (and has no δ-low prefix), only party A sends messages, and again it does so according to the distribution induced by Π.

Since the transcript distribution induced by Π_δ is the same as that of Π, protocol Π_δ is also a coin-flipping protocol. We also note that Π_δ can be implemented efficiently assuming one-way functions do not exist (simply use the inverter of Π's transcript function to estimate the value of a given transcript). Finally, by Equation (5), $\mathsf{A}_\delta^{(i)}$ (i.e., recursive biased-continuation attacks for Π_δ) can be efficiently implemented, since there are *no* low-value transcripts where A needs to send the next message. (Similarly, $\mathsf{B}_\delta^{(i)}$ can be efficiently implemented since there are no high-value transcripts where B needs to send the next message.)

It follows that for any constant $\varepsilon > 0$, there exists constant κ such that either the expected outcome of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is a least $1 - \varepsilon$ or the expected outcome of $(\mathsf{A}_\delta, \mathsf{B}_\delta^{(\kappa)})$ is at most ε. Assume for concreteness that it is the former case. We define our pruning attacker $\mathsf{A}^{(\kappa,\delta)}$ as follows. When playing against B, the attacker $\mathsf{A}^{(\kappa,\delta)}$ acts like $\mathsf{A}_\delta^{(\kappa)}$ would when playing against B_δ. Namely, the attacker pretends that it is in the δ-pruned protocol Π_δ. But once a low- or high-value transcript is reached, $\mathsf{A}^{(\kappa,\delta)}$ acts *honestly* in the rest of the execution (like A would).

It follows that until a low- or high-value transcript has been reached for the first time, the distribution of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is the same as that of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$. Once a δ-low transcript is reached, the expected outcome of both $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ and $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is δ, but when a δ-high transcript is reached, the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is $(1 - \delta)$ (since it plays like A would), where the expected outcome of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$ is at most one. All in all, the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is δ-close to that of $(\mathsf{A}_\delta^{(\kappa)}, \mathsf{B}_\delta)$, and thus the expected outcome of $(\mathsf{A}^{(\kappa,\delta)}, \mathsf{B})$ is at least $1 - \varepsilon - \delta$. Since ε and δ are arbitrary constants, we have established an efficient attacker to bias the outcome of Π by a value that is an arbitrary constant close to one.

1.4 Open Questions

Does the existence of any nontrivial coin-flipping protocol (i.e., bias $\frac{1}{2} - \frac{1}{\mathrm{poly}(n)}$) imply the existence of one-way functions? This is the main question left open. Answering it would fully resolve the computational complexity of coin-flipping protocols.

Article Organization

General notations and definitions used throughout the article are given in Section 2. Our ideal attacker (which has access to a perfect sampler) to bias any coin-flipping protocol is presented and analyzed in Section 3, while in Section 4 we show how to modify the above attacker to be useful when the perfect sampler is replaced with a one-way function inverter.

2 PRELIMINARIES

2.1 Notations

We use lowercase letters for values, uppercase for random variables, uppercase calligraphic letters (e.g., $\mathcal{U}$) to denote sets, boldface for vectors, and uppercase sans-serif (e.g., A) for algorithms (i.e., Turing machines). All logarithms considered here are in base two. Let $\mathbb{N}$ denote the set of natural numbers, where 0 is considered as a natural number, i.e., $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. For $n \in \mathbb{N}$, let $(n) = \{0, \ldots, n\}$, and if n is positive, let $[n] = \{1, \ldots, n\}$, where $[0] = \emptyset$. For $a \in \mathbb{R}$ and $b \geq 0$, let $[a \pm b]$ stand for the interval $[a - b, a + b]$, $(a \pm b]$ for $(a - b, a + b]$, and so forth. We let $\circ$ denote string concatenation. For a nonempty string $t \in \{0,1\}^*$ and $i \in [|t|]$, let t_i be the ith bit of t, and for

$i, j \in [|t|]$ such that $i < j$, let $t_{i,\ldots,j} = t_i \circ t_{i+1} \circ \ldots \circ t_j$. The empty string is denoted by λ, and for a nonempty string, let $t_{1,\ldots,0} = \lambda$. We let poly denote the set all polynomials and let PPTM denote a probabilistic algorithm that runs in *strictly* polynomial time. Given a PPTM algorithm A, we let $\mathsf{A}(u; r)$ be an execution of A on input u given randomness r. A function $\nu : \mathbb{N} \to [0, 1]$ is *negligible*, denoted $\nu(n) = \operatorname{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in$ poly and large enough n.

Given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Similarly, given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution on $\mathcal{S}$. We adopt the convention that when the same random variable occurs several times in an expression, all occurrences refer to a single sample. For example, $\Pr[f(X) = X]$ is defined to be the probability that when $x \leftarrow X$, we have $f(x) = x$. We write U_n to denote the random variable distributed uniformly over $\{0, 1\}^n$. The support of a distribution D over a finite set $\mathcal{U}$, denoted $\operatorname{Supp}(D)$, is defined as $\{u \in \mathcal{U} : D(u) > 0\}$. The *statistical distance* of two distributions P and Q over a finite set $\mathcal{U}$, denoted as $\operatorname{SD}(P, Q)$, is defined as $\max_{\mathcal{S} \subseteq \mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$.

A *measure* is a function $M : \Omega \to [0, 1]$. The support of M over a set Ω, denoted $\operatorname{Supp}(M)$, is defined as $\{\omega \in \Omega : M(\omega) > 0\}$. A measure M over Ω is the *zero measure* if $\operatorname{Supp}(M) = \emptyset$.

2.2 Two-Party Protocols

The following discussion is restricted to no-input (possibly randomized), two-party protocols, where each message consists of a *single* bit. We do not assume, however, that the parties play in turns (i.e., the same party might send two consecutive messages), but only that the protocol's transcript uniquely determines which party is playing next (i.e., the protocol is well defined). In an m-round protocol, the parties exchange exactly m messages (i.e., bits). The tuple of the messages sent so far in any partial execution of a protocol is called the *(communication) transcript* of this execution.

We write that a protocol Π is equal to (A, B) when A and B are the interactive Turing machines that control the left- and right-hand party, respectively, of the interaction according to Π. For a party C interacting according to Π, let $\overline{\mathsf{C}}_\Pi$ be the other party in Π, where if Π is clear from the context, we simply write $\overline{\mathsf{C}}$.

If A and B are deterministic, then $\operatorname{trans}(\mathsf{A}, \mathsf{B})$ denotes the uniquely defined transcript of the protocol (A, B). If A and B are randomized, we let ρ_A and ρ_B be the (maximal) number of random bits used by A and B, respectively. For $r_\mathsf{A} \in \{0, 1\}^{\rho_\mathsf{A}}$, $\mathsf{A}(\cdot; r_\mathsf{A})$ stands for the variant of A when r_A are set as its random coins, and $\mathsf{A}(u; r_\mathsf{A})$ is the message sent by $\mathsf{A}(\cdot; r_\mathsf{A})$ when given a partial transcript u, for which the party A sends the next message. The above notations naturally extend for party B as well. The transcript of the protocol $(\mathsf{A}(\cdot; r_\mathsf{A}), \mathsf{B}(\cdot; r_\mathsf{B}))$ is denoted by $\operatorname{trans}(\mathsf{A}(\cdot; r_\mathsf{A}), \mathsf{B}(\cdot; r_\mathsf{B}))$. For a (partial) transcript u of a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, let $\operatorname{Consis}_\Pi(u)$ be the distribution of choosing $(r_\mathsf{A}, r_\mathsf{B}) \leftarrow \{0, 1\}^{\rho_\mathsf{A}} \times \{0, 1\}^{\rho_\mathsf{B}}$ conditioned on $\operatorname{trans}(\mathsf{A}(\cdot; r_\mathsf{A}), \mathsf{B}(\cdot; r_\mathsf{B}))_{1,\ldots,|u|} = u$.

2.2.1 Binary Trees.

Definition 2.1 (Binary Trees). For $m \in \mathbb{N}$, let $\mathcal{T}^m$ be the complete directed binary tree of height m. We naturally identify the vertices of $\mathcal{T}^m$ with binary strings: the root is denoted by the empty string λ, and the left- and right-hand children of a nonleaf node u are denoted by $u0$ and $u1$, respectively.

- Let $\mathcal{V}(\mathcal{T}^m)$, $\mathcal{E}(\mathcal{T}^m)$, $\operatorname{root}(\mathcal{T}^m)$, and $\mathcal{L}(\mathcal{T}^m)$ denote the vertices, edges, root, and leaves of $\mathcal{T}^m$, respectively.
- For $u \in \mathcal{V}(\mathcal{T}^m) \setminus \mathcal{L}(\mathcal{T}^m)$, let $\mathcal{T}_u^m$ be the subtree of $\mathcal{T}^m$ rooted at u.

- For $u \in \mathcal{V}(\mathcal{T}^m)$, let $\mathrm{desc}_m(u)$ ($\overline{\mathrm{desc}}_m(u)$, respectively) be the descendants of u in $\mathcal{T}^m$ including u (excluding u, respectively), and for $\mathcal{U} \subseteq \mathcal{V}(\mathcal{T}^m)$, let $\mathrm{desc}_m(\mathcal{U}) = \bigcup_{u \in \mathcal{U}} \mathrm{desc}_m(u)$ and $\overline{\mathrm{desc}}_m(\mathcal{U}) = \bigcup_{u \in \mathcal{U}} \overline{\mathrm{desc}}_m(u)$.
- The frontier of a set $\mathcal{U} \subseteq \mathcal{V}(\mathcal{T}^m)$, denoted by $\mathrm{frnt}(\mathcal{U})$, is defined as $\mathcal{U} \setminus \overline{\mathrm{desc}}_m(\mathcal{U})$.[14]

When m is clear from the context, it is typically omitted from the above notation. We will make use of the following simple observations.

Proposition 2.2. *For any subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{V}(\mathcal{T})$, it holds that* $\mathrm{desc}(\mathcal{A}) \subseteq \mathrm{desc}(\mathcal{A} \setminus \overline{\mathrm{desc}}(\mathcal{B})) \cup \mathrm{desc}(\mathcal{B} \setminus \mathcal{A})$.

Proof. Let $u \in \mathrm{desc}(\mathcal{A})$ and let $v \in \mathrm{frnt}(\mathcal{A})$ be such that $u \in \mathrm{desc}(v)$. We show that $v \in \mathrm{desc}(\mathcal{A} \setminus \overline{\mathrm{desc}}(\mathcal{B})) \cup \mathrm{desc}(\mathcal{B} \setminus \mathcal{A})$. Clearly, if $v \notin \overline{\mathrm{desc}}(\mathcal{B})$, we are done. Assume that $v \in \overline{\mathrm{desc}}(\mathcal{B})$, namely, that there exists $w \in \mathcal{B}$ such that $v \in \overline{\mathrm{desc}}(w)$. Since v is in the frontier of $\mathcal{A}$, it follows that $w \notin \mathcal{A}$. Hence, $v \in \mathrm{desc}(\mathcal{B} \setminus \mathcal{A})$, and the proof follows. □

Proposition 2.3. *For any subsets $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ of $\mathcal{V}(\mathcal{T})$, it holds that* $\mathrm{desc}(\mathcal{A}) \subseteq \mathrm{desc}((\mathcal{A} \cup \mathcal{B}) \setminus \mathrm{desc}(\mathcal{C})) \cup \mathrm{desc}(\mathcal{C} \setminus \overline{\mathrm{desc}}(\mathcal{B}))$.

Proof. Let $u \in \mathrm{desc}(\mathcal{A})$ and let $v \in \mathrm{frnt}(\mathcal{A})$ be such that $u \in \mathrm{desc}(v)$. We show that $v \in \mathrm{desc}((\mathcal{A} \cup \mathcal{B}) \setminus \mathrm{desc}(\mathcal{C})) \cup \mathrm{desc}(\mathcal{C} \setminus \overline{\mathrm{desc}}(\mathcal{B}))$. Clearly, if $v \notin \mathrm{desc}(\mathcal{C})$, we are done. Assume that $v \in \mathrm{desc}(\mathcal{C})$, and let $w \in \mathrm{frnt}(\mathcal{C})$ such that $v \in \mathrm{desc}(w)$. If $w \notin \overline{\mathrm{desc}}(\mathcal{B})$, then $w \in \mathcal{C} \setminus \mathrm{desc}(\mathcal{B})$; thus, $v \in \mathrm{desc}(\mathcal{C} \setminus \mathrm{desc}(\mathcal{B}))$ and we are done. Otherwise, if $w \in \overline{\mathrm{desc}}(\mathcal{B})$, then since w is on the frontier of $\mathcal{C}$, it follows that $w \in \mathrm{desc}(\mathcal{B} \setminus \mathrm{desc}(\mathcal{C}))$ and thus also $v \in \mathrm{desc}(\mathcal{B} \setminus \mathrm{desc}(\mathcal{C}))$. The proof follows. □

2.2.2 *Protocol Trees.*

We naturally identify a (possibly partial) transcript of an m-round, single-bit message protocol with a rooted path in $\mathcal{T}^m$. That is, the transcript $t \in \{0,1\}^m$ is identified with the path $\lambda, t_1, t_{1,2}, \ldots, t$.

Definition 2.4 (Tree Representation of a Protocol). We make use of the following definitions with respect to an m-round protocol $\Pi = (\mathsf{A}, \mathsf{B})$, and $\mathsf{C} \in \{\mathsf{A}, \mathsf{B}\}$:

- Let $\mathrm{round}(\Pi) = m$, let $\mathcal{T}(\Pi) = \mathcal{T}^m$, and for $X \in \{\mathcal{V}, \mathcal{E}, \mathrm{root}, \mathcal{L}\}$, let $X(\Pi) = X(\mathcal{T}(\Pi))$.
- The edge distribution induced by a protocol Π is the function $e_\Pi : \mathcal{E}(\Pi) \to [0,1]$, defined as $e_\Pi(u, v)$ being the probability that the transcript of a random execution of Π visits v, conditioned that it visits u.
- For $u \in \mathcal{V}(\Pi)$, let $\mathrm{v}_\Pi(u) = e_\Pi(\lambda, u_1) \cdot e_\Pi(u_1, u_{1,2}) \ldots \cdot e_\Pi(u_{1,\ldots,|u|-1}, u)$, and let the leaf distribution induced by Π be the distribution $\langle \Pi \rangle$ over $\mathcal{L}(\Pi)$, defined by $\langle \Pi \rangle(u) = \mathrm{v}_\Pi(u)$.
- The party that sends the next message on transcript u is said to control u, and we denote this party by $\mathrm{cntrl}_\Pi(u)$. We call $\mathrm{cntrl}_\Pi : \mathcal{V}(\Pi) \to \{\mathsf{A}, \mathsf{B}\}$ the control scheme of Π. Let $\mathcal{C}\mathrm{trl}_\Pi^{\mathsf{C}} = \{u \in \mathcal{V}(\Pi) : \mathrm{cntrl}_\Pi(u) = \mathsf{C}\}$.

For $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, let $\Pr_{\langle \Pi \rangle}[\mathcal{S}]$ be an abbreviation for $\Pr_{\ell \leftarrow \langle \Pi \rangle}[\ell \in \mathcal{S}]$. Note that every function $e : \mathcal{E}(\mathcal{T}^m) \to [0,1]$ with $e(u, u0) + e(u, u1) = 1$ for every $u \in \mathcal{V}(\mathcal{T}^m) \setminus \mathcal{L}(\mathcal{T}^m)$ with $\mathrm{v}(u) > 0$, along with a control scheme (active in each node), defines a two-party, m-round, single-bit message protocol (the resulting protocol might be inefficient). The analysis in Section 3 naturally gives rise to functions over binary trees that do not correspond to any two-party execution. We identify

[14] This is the set of all "maximal" transcripts in $\mathcal{U}$ under the partial-order subsequence relation.

the "protocols" induced by such functions by the special symbol $\perp$. We let $\mathrm{E}_{\langle\perp\rangle}[f] = 0$, for any real-value function f.

The view of a protocol as an edge distribution function allows us to consider protocols induced by subtrees of $\mathcal{T}(\Pi)$.

Definition 2.5 (Subprotocols). Let Π be a protocol and let $u \in \mathcal{V}(\Pi)$. Let $(\Pi)_u$ denote the protocol induced by the function e_Π on the subtree of $\mathcal{T}(\Pi)$ rooted at u, if $\mathrm{v}_\Pi(u) > 0$, and let $(\Pi)_u = \perp$ otherwise.

Namely, the protocol $(\Pi)_u$ is the protocol Π conditioned on u being the transcript of the first $|u|$ rounds. When convenient, we remove the parentheses from notation, and simply write Π_u. Two subprotocols of interest are Π_0 and Π_1, induced by e_Π and the trees rooted at the left- and right-hand descendants of $\mathsf{root}(\mathcal{T})$. For a measure $M : \mathcal{L}(\Pi) \to [0,1]$ and $u \in \mathcal{V}(\Pi)$, let $(M)_u : \mathcal{L}(\Pi_u) \to [0,1]$ be the restricted measure induced by M on the subprotocol Π_u. Namely, for any $\ell \in \mathcal{L}(\Pi_u)$, $(M)_u(\ell) = M(\ell)$.

2.2.3 Tree Value.

Definition 2.6 (Tree Value). Let Π be a two-party protocol in which at the end of any of its executions, the parties output the same real value. Let $\chi_\Pi : \mathcal{L}(\Pi) \to \mathbb{R}$ be the common output function of Π — $\chi_\Pi(\ell)$ is the common output of the parties in an execution ending in ℓ.[15] Let $\mathsf{val}(\Pi) = \mathrm{E}_{\langle\Pi\rangle}[\chi_\Pi]$, and for $x \in \mathbb{R}$, let $\mathcal{L}_x(\Pi) = \{\ell \in \mathcal{L}(\Pi) : \chi_\Pi(\ell) = x\}$.

Throughout this article, we restrict ourselves to protocols whose common output is either one or zero; i.e., the image of χ_Π is the set $\{0,1\}$. The following immediate fact states that the expected value of a measure, whose support is a subset of the 1-leaves of some protocol, is always smaller than the value of that protocol.

Fact 2.7. *Let Π be a protocol and let M be a measure over $\mathcal{L}_1(\Pi)$. Then $\mathrm{E}_{\langle\Pi\rangle}[M] \le \mathsf{val}(\Pi)$.*

We will also make use of the following proposition, showing that if two protocols are close and there exists a set of nodes whose value (the probability that the common output is one conditioned on reaching these nodes) is large in one protocol but small in the other, then the probability of reaching this set is small.

Proposition 2.8. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ and $\Pi' = (\mathsf{C}, \mathsf{D})$ be two m-round protocols with $\chi_\Pi \equiv \chi_{\Pi'}$, and let $\mathcal{F} \subseteq \mathcal{V}(\Pi)$ be a frontier. Assume that $SD(\langle\Pi\rangle, \langle\Pi'\rangle) \le \varepsilon$, that $\Pr_{\langle\Pi\rangle}[\mathcal{L}_1(\Pi) \mid \mathsf{desc}(\mathcal{F})] \le \alpha$, and that $\Pr_{\langle\Pi'\rangle}[\mathcal{L}_1(\Pi) \mid \mathsf{desc}(\mathcal{F})] \ge \beta$, for some $\varepsilon > 0$ and $0 \le \alpha < \beta \le 1$. Then, $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{F})] \le \varepsilon \cdot \frac{1+\beta}{\beta-\alpha}$.*

Note that since both Π and Π' have m-rounds, it holds that $\mathcal{V}(\Pi) = \mathcal{V}(\Pi')$ and $\mathcal{L}(\Pi) = \mathcal{L}(\Pi')$. Moreover, since $\chi_\Pi \equiv \chi_{\Pi'}$, it also holds that $\mathcal{L}_1(\Pi)$, the set of 1-leaves in Π, is identical to $\mathcal{L}_1(\Pi')$, the set of 1-leaves in Π'.

Proof. Let $\mu = \Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{F})]$, $\mu' = \Pr_{\langle\Pi'\rangle}[\mathsf{desc}(\mathcal{F})]$ and $\mathcal{S} = \mathcal{L}_1(\Pi) \cap \mathsf{desc}(\mathcal{F})$. It follows that

$$\Pr_{\langle\Pi\rangle}[\mathcal{S}] = \Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{F})] \cdot \Pr_{\langle\Pi\rangle}[\mathcal{L}_1(\Pi) \mid \mathsf{desc}(\mathcal{F})] \le \mu \cdot \alpha \tag{6}$$

[15] Conditioned that an execution of the protocol generates a transcript ℓ, the parties' coins are in a product distribution. Hence, if the parties always have the same output, then the protocol's output is indeed a (deterministic) function of its transcript.

and that

$$\Pr_{\langle\Pi'\rangle}[\mathcal{S}] = \Pr_{\langle\Pi'\rangle}[\mathrm{desc}(\mathcal{F})] \cdot \Pr_{\langle\Pi'\rangle}[\mathcal{L}_1(\Pi) \mid \mathrm{desc}(\mathcal{F})] \geq \mu' \cdot \beta. \tag{7}$$

Moreover, since $\mathrm{SD}(\langle\Pi\rangle, \langle\Pi'\rangle) \leq \varepsilon$, it follows that $\mu' \geq \mu - \varepsilon$ and that $\Pr_{\langle\Pi'\rangle}[\mathcal{S}] - \Pr_{\langle\Pi\rangle}[\mathcal{S}] \leq \varepsilon$. Putting it all together, we get

$$\begin{aligned} \varepsilon &\geq \Pr_{\langle\Pi'\rangle}[\mathcal{S}] - \Pr_{\langle\Pi\rangle}[\mathcal{S}] \\ &\geq \mu' \cdot \beta - \mu \cdot \alpha \\ &\geq (\mu - \varepsilon) \cdot \beta - \mu \cdot \alpha \\ &= (\beta - \alpha) \cdot \mu - \beta \cdot \varepsilon, \end{aligned}$$

which implies the proposition. □

2.2.4 Protocol with Common Inputs. We sometimes would like to apply the above terminology to a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ whose parties get a common security parameter 1^n. This is formally done by considering the protocol $\Pi_n = (\mathsf{A}_n, \mathsf{B}_n)$, where C_n is the algorithm derived by "hardwiring" 1^n into the code of C.

2.3 Coin-Flipping Protocols

In a coin-flipping protocol, two parties interact and in the end have a common output bit. Ideally, this bit should be random and no cheating party should be able to bias its outcome to either direction (if the other party remains honest). For interactive, probabilistic algorithms A and B, and $x \in \{0,1\}^*$, let $\mathrm{out}(\mathsf{A},\mathsf{B})(x)$ denote the parties' output, on common input x.

Definition 2.9 ((Strong) Coin Flipping). A PPT protocol (A, B) is a δ-bias coin-flipping protocol if the following holds.

Correctness: $\Pr[\mathrm{out}(\mathsf{A},\mathsf{B})(1^n) = 0] = \Pr[\mathrm{out}(\mathsf{A},\mathsf{B})(1^n) = 1] = \frac{1}{2}$.
Security: $\Pr[\mathrm{out}(\mathsf{A}^*,\mathsf{B})(1^n) = c], \Pr[\mathrm{out}(\mathsf{A},\mathsf{B}^*)(1^n) = c] \leq \frac{1}{2} + \delta(n)$, for any PPTM A^* and B^*, bit $c \in \{0,1\}$, and large enough n.

Sometimes, e.g., if the parties have (a priori known) opposite preferences, an even weaker definition of coin-flipping protocols is of interest.

Definition 2.10 (Weak Coin Flipping). A PPT protocol (A, B) is a weak δ-bias coin-flipping protocol if the following holds.

Correctness: Same as in Definition 2.9.
Security: There exist bits $c_{\mathsf{A}} \neq c_{\mathsf{B}} \in \{0,1\}$ such that

$$\Pr[\mathrm{out}(\mathsf{A}^*,\mathsf{B})(1^n) = c_{\mathsf{A}}], \Pr[\mathrm{out}(\mathsf{A},\mathsf{B}^*)(1^n) = c_{\mathsf{B}}] \leq \frac{1}{2} + \delta(n)$$

for any PPTM A^* and B^*, and large enough n.

Remark 2.11. Our result still holds when allowing the common bit in a random honest execution of the protocol to be an arbitrary constant in $(0,1)$. In contrast, our proof critically relies on the assumption that the honest parties are *always* in agreement.

In the rest of the article, we restrict our attention to m-round single-bit message coin-flipping protocols, where $m = m(n)$ is a function of the protocol's security parameter. Given such a protocol $\Pi = (\mathsf{A},\mathsf{B})$, we assume that its common output (i.e., the coin) is efficiently computable from a (full) transcript of the protocol. (It is easy to see that these assumptions are without loss of generality.)

2.4 One-Way Functions and Distributional One-Way Functions

A one-way function (OWF) is an efficiently computable function whose inverse cannot be computed on average by any PPTM.

Definition 2.12. A polynomial-time computable function $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is one-way if

$$\Pr_{x \leftarrow \{0,1\}^n; y=f(x)}\left[\mathsf{A}(1^n, y) \in f^{-1}(y)\right] = \operatorname{neg}(n)$$

for any PPTM A.

A seemingly weaker definition is that of a distributional OWF. Such a function is easy to compute, but it is hard to compute uniformly random preimages of random images.

Definition 2.13. A polynomial-time computable $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is distributional one-way, if $\exists p \in \operatorname{poly}$ such that

$$\mathsf{SD}\left((x, f(x))_{x \leftarrow \{0,1\}^n}, (\mathsf{A}(f(x)), f(x))_{x \leftarrow \{0,1\}^n}\right) \geq \frac{1}{p(n)}$$

for any PPTM A and large enough n.

Clearly, any one-way function is also a distributional one-way function. While the other implication is not necessarily always true, Impagliazzo and Luby [16] showed that the existence of distributional one-way functions implies that of (standard) one-way functions. In particular, the authors of [16] proved that if one-way functions do not exist, then any efficiently computable function has an inverter of the following form.

Definition 2.14 (ξ-inverter). An algorithm Inv is an ξ-inverter of $f : \mathcal{D} \to \mathcal{R}$ if the following holds:

$$\Pr_{x \leftarrow \mathcal{D}; y=f(x)}\left[\mathsf{SD}\left((x')_{x' \leftarrow f^{-1}(y)}, (\mathsf{Inv}(y))\right) > \xi\right] \leq \xi.$$

Lemma 2.15 ([16, Lemma 1]). *Assume one-way functions do not exist. Then for any polynomial-time computable function $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ and $p \in \operatorname{poly}$, there exists a PPTM algorithm Inv such that the following holds for infinitely many n's. On security parameter 1^n, algorithm Inv is a $1/p(n)$-inverter of f_n (i.e., f is restricted to $\{0,1\}^n$).*

Impagliazzo and Luby [16] only gave a proof sketch for the above lemma. The full proof can be found in [15, Theorem 4.2.2].

Remark 2.16 (Definition of Inverter). In their original definition, Impagliazzo and Luby [16] defined a ξ-inverter as an algorithm Inv for which it holds that

$$\mathsf{SD}\left((x, f(x))_{x \leftarrow \{0,1\}^n}, (\mathsf{Inv}(f(x)), f(x))_{x \leftarrow \{0,1\}^n}\right) < \xi.$$

They also proved Lemma 2.15 with respect to this definition. By taking, for example, $\xi' = \xi^2$ and applying their proof with ξ', it is easy to see how our version of Lemma 2.15 follows with respect to the above definition of a ξ-inverter.

Note that nothing is guaranteed when invoking a good inverter (i.e., a γ-inverter for some small γ) on an *arbitrary distribution*. Yet the following lemma yields that if the distribution in consideration is "not too different" from the output distribution of f, then such good inverters are useful.

Lemma 2.17. *Let f and g be two randomized functions over the same domain $\mathcal{D} \cup \{\perp\}$ such that $f(\perp) \equiv g(\perp)$, and let $\{P_i\}_{i\in[k]}$ be a set of distributions over $\mathcal{D} \cup \{\perp\}$ such that for some $a \geq 0$, it holds that $\mathrm{E}_{q\leftarrow P_i}[SD(f(q), g(q))] \leq a$ for every $i \in [k]$. Let A be a k-query oracle-aided algorithm that only makes queries in $\mathcal{D}$. Let $Q = (Q_1, \ldots, Q_k)$ be the random variable of the queries of A^f in such a random execution, setting $Q_i =\perp$ if A makes less than i queries.*

Assume that $\Pr_{(q_1,\ldots,q_k)\leftarrow Q}[\exists i \in [k] : q_i \neq\perp \wedge Q_i(q_i) > \lambda \cdot P_i(q_i)] \leq b$ for some $\lambda, b \geq 0$. Then $SD(\mathsf{A}^f, \mathsf{A}^g) \leq b + ka\lambda$.

To prove Lemma 2.17, we use the following proposition.

Proposition 2.18. *For every two distributions P and Q over a set $\mathcal{D}$, there exists a distribution $R_{P,Q}$ over $\mathcal{D} \times \mathcal{D}$, such that the following hold:*

(1) $(R_{P,Q})_1 \equiv P$ and $(R_{P,Q})_2 \equiv Q$, where $(R_{P,Q})_b$ is the projection of $R_{P,Q}$ into its bth coordinate.
(2) $\Pr_{(x_1,x_2)\leftarrow R_{P,Q}}[x_1 \neq x_2] = SD(P, Q)$.

Proof. For every $x \in \mathcal{D}$, let $M(x) = \min\{P(x), Q(x)\}$, $M_P(x) = P(x) - M(x)$, and $M_Q(x) = Q(x) - M(x)$. The distribution $R_{P,Q}$ is defined by the following procedure. With probability $\mu = \sum_{x\in\mathcal{D}} M(x)$, sample an element x according to M (i.e., x is returned with probability $\frac{M(x)}{\mu}$), and return (x, x); otherwise, return (x_P, x_Q), where x_P is sampled according to M_P and x_Q is sampled according to M_Q. It is clear that $\Pr_{(x_1,x_2)\leftarrow R_{P,Q}}[x_1 \neq x_2] = \mathrm{SD}(P, Q)$. It also holds that

$$\begin{aligned}(R_{P,Q})_1(x) &= \mu \cdot \frac{M(x)}{\mu} + (1-\mu) \cdot \frac{M_P(x)}{\mu_P}\\ &= M(x) + M_P(x)\\ &= P(x),\end{aligned}$$

where $\mu_P := \sum_{x\in\mathcal{D}} M_P = (1 - \mu)$. Namely, $(R_{P,Q})_1 \equiv P$. The proof that $(R_{P,Q})_2 \equiv Q$ is analogous. □

Proof of Lemma 2.17. Using Proposition 2.18 and standard argument, it holds that $\mathrm{SD}(\mathsf{A}^f, \mathsf{A}^g)$ is at most the probability that the following experiment aborts.

Experiment 2.19.

(1) Start emulating a random execution of A.
(2) Do until A halts:
  (a) Let q be the next query of A.
  (b) Sample $(a_1, a_2) \leftarrow R_{f(q),g(q)}$.
  (c) If $a_1 = a_2$, give a_1 to A as the oracle answer.
  Otherwise, abort.

By setting $\mathcal{S}_i = \{q : q \in \mathrm{Supp}(Q_i) \wedge Q_i(q) \leq \lambda \cdot P_i(q)\}$ for $i \in [k]$ and recalling that by assumption $f(\perp) \equiv g(\perp)$ (thus, when sampling $(a_1, a_2) \leftarrow R_{f(\perp),g(\perp)}$, a_1 always equals a_2), we conclude that

$$\begin{aligned}
\mathrm{SD}(\mathrm{A}^f, \mathrm{A}^g) &\leq \Pr_{(q_1,\ldots,q_k)\leftarrow Q}[\exists i \in [k] : q_i \notin \mathcal{S}_i \cup \{\perp\}] \\
&\quad + \Pr_{(q_1,\ldots,q_k)\leftarrow Q}\left[\exists i \in [k] : a_1 \neq a_2 \text{ where } (a_1,a_2) \leftarrow R_{f(q_i),g(q_i)} \wedge q_i \in \mathcal{S}_i\right] \\
&\leq b + \sum_{i\in[k]} \sum_{q\in\mathcal{S}_i} Q_i(q) \cdot \Pr\left[a_1 \neq a_2 \text{ where } (a_1,a_2) \leftarrow R_{f(q),g(q)}\right] \\
&\overset{(1)}{\leq} b + \sum_{i\in[k]} \sum_{q\in\mathcal{S}_i} Q_i(q) \cdot \mathrm{SD}(f(q), g(q)) \\
&\overset{(2)}{\leq} b + \sum_{i\in[k]} \sum_{q\in\mathrm{Supp}(P_i)} \lambda \cdot P_i(q) \cdot \mathrm{SD}(f(q), g(q)) \\
&\leq b + \lambda \sum_{i\in[k]} \mathrm{E}_{q\leftarrow P_i}[\mathrm{SD}(f(q), g(q))] \\
&\leq b + ka\lambda,
\end{aligned}$$

where (1) follows from Proposition 2.18 and (2) from the definition of the sets $\{S_i\}_{i\in[k]}$. □

2.5 Two Inequalities

We make use of the following technical lemmas, whose proofs are given in Appendix A.

Lemma 2.20. *Let $x, y \in [0,1]$, let $k \geq 1$ be an integer, and let $a_1,\ldots,a_k,b_1,\ldots,b_k \in (0,1]$. Then for any $p_0, p_1 \geq 0$ with $p_0 + p_1 = 1$, it holds that*

$$p_0 \cdot \frac{x^{k+1}}{\prod_{i=1}^k a_i} + p_1 \cdot \frac{y^{k+1}}{\prod_{i=1}^k b_i} \geq \frac{(p_0 x + p_1 y)^{k+1}}{\prod_{i=1}^k (p_0 a_i + p_1 b_i)}.$$

Lemma 2.21. *For every $\delta \in (0, \frac{1}{2}]$, there exists $\alpha = \alpha(\delta) \in (0,1]$ such that*

$$\lambda \cdot a_1^{1+\alpha} \cdot (2 - a_1 \cdot x) + a_2^{1+\alpha} \cdot (2 - a_2 \cdot x) \leq (1+\lambda) \cdot (2 - x)$$

for every $x \geq \delta$ and $\lambda, y \geq 0$ with $\lambda y \leq 1$, for $a_1 = 1 + y$ and $a_2 = 1 - \lambda y$.

3 THE BIASED-CONTINUATION ATTACK

In this section, we describe an attack to bias any coin-flipping protocol. The described attack, however, might be impossible to implement efficiently (even when assuming one-way functions do not exist). Specifically, we assume access to an ideal sampling algorithm to sample a *uniform* preimage of *any* output of the functions under consideration. Our actual attack, the subject of Section 4, tries to mimic the behavior of this attack while being efficiently implemented (assuming one-way functions do not exist).

The following discussion is restricted to (coin-flipping) protocols whose parties always output the same bit as their common output, and this bit is determined by the protocol's transcript. In all protocols considered in this section, the messages are bits. In addition, the protocols under consideration have no inputs (neither private nor common), and in particular no security parameter is involved.[16] Recall that $\perp$ stands for a canonical invalid/undefined protocol, and that $\mathrm{E}_{\langle\perp\rangle}[f] = 0$, for any real value function f. (We refer the reader to Section 2 for a discussion of the conventions and assumptions used above.) Although the focus of this article is coin-flipping protocols,

[16] In Section 4, we make use of these inputless protocols by "hardwiring" the security parameter of the protocols under consideration.

all the results in this section hold true for any two-party protocol meeting the above assumptions. Specifically, we do not assume that an honest execution of the protocol produces a uniformly random bit, nor do we assume that the parties executing the protocol can be implemented by a polynomial-time probabilistic Turing machine. For this reason we omit the term "coin flipping" in this section.

Throughout the section, we prove statements with respect to attackers that, when playing the role of the left-hand party of the protocol (i.e., A), are trying to bias the common output of the protocol toward one, and, when playing the role of the right-hand party of the protocol (i.e., B), are trying to bias the common output of the protocol toward zero. All statements have analog ones with respect to the opposite attack goals.

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol. The *recursive biased-continuation attack* described below recursively applies the *biased-continuation attack* introduced by Haitner and Omri [13].[17] The biased-continuation attacker $\mathsf{A}_\Pi^{(1)}$—playing the role of A—works as follows: in each of A's turns, $\mathsf{A}_\Pi^{(1)}$ picks a random continuation of Π, whose output it induces is equal to one, and plays the current turn accordingly. The ith biased-continuation attacker $\mathsf{A}_\Pi^{(i)}$, formally described below, uses the same strategy but the random continuation taken is of the protocol $(\mathsf{A}_\Pi^{(i-1)}, \mathsf{B})$.

Moving to the formal discussion, for a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, we defined its biased continuator $\mathsf{BiasedCont}_\Pi$ as follows.

Definition 3.1 (Biased Continuator $\mathsf{BiasedCont}_\Pi$*).*

```
Input: $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$ and a bit $b \in \{0, 1\}$
Operation:
  (1) Choose $\ell \leftarrow \langle \Pi \rangle$ conditioned that
      (a) $\ell \in \mathrm{desc}(u)$, and
      (b) $\chi_\Pi(\ell) = b$.[18]
  (2) Return $\ell_{|u|+1}$.
```

Let $\mathsf{A}_\Pi^{(0)} \equiv \mathsf{A}$, and for integer $i > 0$ define:

Algorithm 3.2 (Recursive Biased-continuation Attacker $\mathsf{A}_\Pi^{(i)}$).

```
*Input: transcript* $u \in \{0, 1\}^*$.
*Operation:*
  (1) *If* $u \in \mathcal{L}(\Pi)$, *output* $\chi_\Pi(u)$ *and halt.*
  (2) *Set* $\mathsf{msg} = \mathsf{BiasedCont}_{(\mathsf{A}_\Pi^{(i-1)}, \mathsf{B})}(u, 1)$.
  (3) *Send* $\mathsf{msg}$ *to* $\mathsf{B}$.
  (4) *If* $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$, *output* $\chi_\Pi(u')$.[19]
```

The attacker $\mathsf{B}_\Pi^{(i)}$ attacking toward zero is analogously defined (specifically, the call to the biased continuator $\mathsf{BiasedCont}_{(\mathsf{A}_\Pi^{(i-1)}, \mathsf{B})}(u, 1)$ in Algorithm 3.2 is changed to $\mathsf{BiasedCont}_{(\mathsf{A}, \mathsf{B}_\Pi^{(i-1)})}(u, 0)$).[20]

It is relatively easy to show that the more recursions $\mathsf{A}_\Pi^{(i)}$ and $\mathsf{B}_\Pi^{(i)}$ do, the closer their success probability is to that of an all-powerful attacker, who can bias the outcome either to zero or to one.

[17] Called the "random continuation attack" in [13].

[18] If no such ℓ exists, the algorithm returns an arbitrary leaf in $\mathrm{desc}(u)$.

[19] For the mere purpose of biasing B's output, there is no need for $\mathsf{A}^{(i)}$ to output anything. Yet doing so helps us to simplify our recursion definitions (specifically, we use the fact that in $(\mathsf{A}^{(i)}, \mathsf{B})$, the parties always have the same output).

[20] The subscript Π is added to the notation (i.e., $\mathsf{A}_\Pi^{(i)}$), since the biased-continuation attack for A depends not only on the definition of the party A but also on the definition of B, the other party in the protocol.

The important point of the following theorem is that, for any $\varepsilon > 0$, there exists a *global* constant $\kappa = \kappa(\varepsilon)$ (i.e., independent of the underlying protocol), for which either $\mathsf{A}_{\Pi}^{(\kappa)}$ or $\mathsf{B}_{\Pi}^{(\kappa)}$ succeeds in its attack with probability at least $1 - \varepsilon$. This becomes crucial when trying to efficiently implement these adversaries (see Section 4), as each recursion call might induce a polynomial blowup in the running time of the adversary. Since κ is constant (for a constant ε), the recursive attacker is still efficient.

Theorem 3.3 (Main Theorem, Ideal Version). *For every $\varepsilon \in (0, \frac{1}{2}]$, there exists nonnegative integer $\kappa \in \widetilde{O}(1/\varepsilon)$ such that for every protocol $\Pi = (\mathsf{A}, \mathsf{B})$, either $\mathsf{val}(\mathsf{A}_{\Pi}^{(\kappa)}, \mathsf{B}) > 1 - \varepsilon$ or $\mathsf{val}(\mathsf{A}, \mathsf{B}_{\Pi}^{(\kappa)}) < \varepsilon$.*

The rest of this section is devoted to proving the above theorem.

In what follows, we typically omit the subscript Π from the notation of the above attackers. Toward proving Theorem 3.3, we show a strong (and somewhat surprising) connection between recursive biased-continuation attacks on a given protocol and the optimal valid attack on this protocol. The latter is the best (unbounded) attack on this protocol, which sends only valid messages (ones that could have been sent by the honest party). Toward this goal, we define sequences of measures over the leaves (i.e., transcripts) of the protocol, connect these measures to the optimal attack, and then lower bound the success of the recursive biased-continuation attacks using these measures.

In the following, we first observe some basic properties of the recursive biased-continuation attack. Next, we define the optimal valid attack, define a simple measure with respect to this attack, and analyze, as a warmup, the success of recursive biased-continuation attacks on this measure. After arguing why considering the latter measure does not suffice, we define a sequence of measures and then state, in Section 3.6, a property of this sequence that yields Theorem 3.3 as a corollary. The main body of this section deals with proving the aforementioned property.

3.1 Basic Observations About $\mathsf{A}^{(i)}$

We make two basic observations regarding the recursive biased-continuation attack. The first gives expression to the edge distribution this attack induces. The second is that this attack is stateless. We'll use these observations in the following sections; however, the reader might want to skip the straightforward proofs for now.

Recall that at each internal node in its control, $\mathsf{A}^{(1)}$ picks a random continuation to one. We can also describe $\mathsf{A}^{(1)}$'s behavior as follows: after seeing a transcript u, $\mathsf{A}^{(1)}$ biases the probability of sending, e.g., 0 to B: it does so proportionally to the ratio between the chance of having output one among all honest executions of the protocol that are consistent with the transcript $u \circ 0$, and the same chance but with respect to the transcript u. The behavior of $\mathsf{A}^{(i)}$ is analogous where $\mathsf{A}^{(i-1)}$ replaces the role of A in the above discussion. Formally, we have the following claim.

Claim 3.4. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and let $\mathsf{A}^{(j)}$ be according to Algorithm 3.2. Then*

$$e_{(\mathsf{A}^{(i)},\mathsf{B})}(u, ub) = e_{\Pi}(u, ub) \cdot \frac{\prod_{j=0}^{i-1} \mathsf{val}((\mathsf{A}^{(j)}, \mathsf{B})_{ub})}{\prod_{j=0}^{i-1} \mathsf{val}((\mathsf{A}^{(j)}, \mathsf{B})_{u})},^{21}$$

for any $i \in \mathbb{N}$, A-controlled $u \in \mathcal{V}(\Pi)$, and $b \in \{0, 1\}$.

[21] Recall that for a protocol Π and a partial transcript u, we let $e_{\Pi}(u, ub)$ stand for the probability that the party controlling u sends b as the next message, conditioning that u is the transcript of the execution thus far.

This claim is a straightforward generalization of the proof of [13, Lemma 12]. However, for completeness and to give an example of our notations, a full proof is given below.

Proof. The proof is by induction on i. For $i = 0$, recall that $\mathsf{A}^{(0)} \equiv \mathsf{A}$, and hence $e_{(\mathsf{A}^{(0)},\mathsf{B})}(u, ub) = e_{\Pi}(u, ub)$, as required.

Assume the claim holds for $i - 1$, and we want to compute $e_{(\mathsf{A}^{(i)},\mathsf{B})}(u, ub)$. The definition of Algorithm 3.2 yields that for any positive $i \in \mathbb{N}$, it holds that

$$\begin{aligned} e_{(\mathsf{A}^{(i)},\mathsf{B})}(u,ub) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B}\rangle}\left[\ell_{|u|+1} = b \;\middle|\; \ell \in \mathsf{desc}(u) \wedge \chi_{(\mathsf{A}^{(i-1)},\mathsf{B})}(\ell) = 1\right]^{22} \quad (8) \\ &= \frac{\Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B}\rangle}\left[\ell_{|u|+1} = b \wedge \chi_{(\mathsf{A}^{(i-1)},\mathsf{B})}(\ell) = 1 \;\middle|\; \ell \in \mathsf{desc}(u)\right]}{\Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B}\rangle}\left[\chi_{(\mathsf{A}^{(i-1)},\mathsf{B})}(\ell) = 1 \;\middle|\; \ell \in \mathsf{desc}(u)\right]} \\ &= e_{(\mathsf{A}^{(i-1)},\mathsf{B})}(u,ub) \cdot \frac{\mathsf{val}((\mathsf{A}^{(i-1)},\mathsf{B})_{ub})}{\mathsf{val}((\mathsf{A}^{(i-1)},\mathsf{B})_{u})}, \end{aligned}$$

where the last equality is by a simple chain rule, i.e., since

$$\begin{aligned} e_{(\mathsf{A}^{(i-1)},\mathsf{B})}(u,ub) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B}\rangle}\left[\ell_{|u|+1} = b \;\middle|\; \ell \in \mathsf{desc}(u)\right], \text{ and} \\ \mathsf{val}((\mathsf{A}^{(i-1)},\mathsf{B})_{ub}) &= \Pr_{\ell \leftarrow \langle \mathsf{A}^{(i-1)},\mathsf{B}\rangle}\left[\chi_{(\mathsf{A}^{(i-1)},\mathsf{B})}(\ell) = 1 \;\middle|\; \ell \in \mathsf{desc}(u) \wedge \ell_{|u|+1} = b\right]. \end{aligned}$$

The proof is concluded by plugging the induction hypothesis into Equation (8). □

The following observation enables us to use induction when analyzing the power of $\mathsf{A}^{(i)}$.

Proposition 3.5. *For every protocol* $\Pi = (\mathsf{A}_\Pi, \mathsf{B}_\Pi)$, $i \in \mathbb{N}$, *and* $b \in \{0, 1\}$, *it holds that* $(\mathsf{A}_\Pi^{(i)}, \mathsf{B})_b$ *and* $(\mathsf{A}_{\Pi_b}^{(i)}, \mathsf{B}_{\Pi_b})$ *are the same protocol, where* $\Pi_b = (\mathsf{A}_{\Pi_b}, \mathsf{B}_{\Pi_b})$.

Proof. Immediately follows from $\mathsf{A}_\Pi^{(i)}$ being stateless. □

Remark 3.6. Note that the party B_{Π_b}, defined by the subprotocol Π_b (specifically, by the edge distribution of the subtree $\mathcal{T}(\Pi_b)$), might not have an efficient implementation, even if B does have one. For the sake of the arguments we make in this section, however, it matters only that B_{Π_b} is well defined.

3.2 Optimal Valid Attacks

When considering the optimal attackers for a given protocol, we restrict ourselves to valid attackers. Informally, we can say that, on each of its turns, a valid attacker sends a message from the set of possible replies that the honest party might choose given the transcript so far.

Definition 3.7 (Optimal Valid Attacker). Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol. A deterministic algorithm A' playing the role of A in Π is in $\mathcal{A}^*$, if $\mathsf{v}_\Pi(u) = 0 \Rightarrow \mathsf{v}_{(\mathsf{A}',\mathsf{B})}(u) = 0$ for any $u \in \mathcal{V}(\Pi)$. The class $\mathcal{B}^*$ is analogously defined. Let $\mathsf{OPT}_\mathsf{A}(\Pi) = \max_{\mathsf{A}' \in \mathcal{A}^*}\{\mathsf{val}(\mathsf{A}', \mathsf{B})\}$ and $\mathsf{OPT}_\mathsf{B}(\Pi) = \max_{\mathsf{B}' \in \mathcal{B}^*}\{1 - \mathsf{val}(\mathsf{A}, \mathsf{B}')\}$.

The following proposition is immediate.

[22] Recall that for a protocol Π, we let $\langle\Pi\rangle$ stand for the leaf distribution of Π.

Proposition 3.8. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol and let* $u \in \mathcal{V}(\Pi)$. *Then,*

$$\mathsf{OPT}_\mathsf{A}(\Pi_u) = \begin{cases} \chi_\Pi(u) & u \in \mathcal{L}(\Pi); \\ \max\{\mathsf{OPT}_\mathsf{A}(\Pi_{ub}) : e_\Pi(u, ub) > 0\} & u \notin \mathcal{L}(\Pi) \text{ and } u \text{ is controlled by } \mathsf{A}; \\ e_\Pi(u, u0) \cdot \mathsf{OPT}_\mathsf{A}(\Pi_{u0}) & u \notin \mathcal{L}(\Pi) \text{ and } u \text{ is controlled by } \mathsf{B}, \\ \quad + e_\Pi(u, u1) \cdot \mathsf{OPT}_\mathsf{A}(\Pi_{u1}) & \end{cases}$$

and the analog conditions hold for $\mathsf{OPT}_\mathsf{B}(\Pi_u)$.[23]

The following holds true for any (bit value) protocol.

Proposition 3.9. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) \in [0, 1]$. *Then either* $\mathsf{OPT}_\mathsf{A}(\Pi)$ *or* $\mathsf{OPT}_\mathsf{B}(\Pi)$ *(but not both) is equal to 1.*

The somewhat surprising part is that *only* one party has a valid winning strategy. Assume for simplicity that $\mathsf{OPT}_\mathsf{A}(\Pi) = 1$. Since A might accidentally mimic the optimal winning valid attacker, it follows that for any valid strategy B' for B there is a positive probability over the random choices of the honest A that the outcome is *not* zero. Namely, it holds that $\mathsf{OPT}_\mathsf{B}(\Pi) < 1$. The formal proof follows a straightforward induction on the protocol's round complexity.

Proof of Proposition 3.9. The proof is by induction on the round complexity of Π. Assume that $\mathsf{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. If $\chi_\Pi(\ell) = 1$, the proof follows since $\mathsf{OPT}_\mathsf{A}(\Pi) = 1$ and $\mathsf{OPT}_\mathsf{B}(\Pi) = 0$. In the complementary case, i.e., $\chi_\pi(\ell) = 0$, the proof follows since $\mathsf{OPT}_\mathsf{A}(\Pi) = 0$ and $\mathsf{OPT}_\mathsf{B}(\Pi) = 1$.

Assume that the lemma holds for m-round protocols and that $\mathsf{round}(\Pi) = m + 1$. If $e_\Pi(\lambda, b) = 1$[24] for some $b \in \{0, 1\}$, since Π is a protocol, it holds that $e_\Pi(\lambda, 1 - b) = 0$. Hence, by Proposition 3.8, it holds that $\mathsf{OPT}_\mathsf{A}(\Pi) = \mathsf{OPT}_\mathsf{A}(\Pi_b)$ and $\mathsf{OPT}_\mathsf{B}(\Pi) = \mathsf{OPT}_\mathsf{B}(\Pi_b)$, regardless of the party controlling $\mathsf{root}(\Pi)$. The proof follows from the induction hypothesis.

If $e_\Pi(\lambda, b) \notin \{0, 1\}$ for both $b \in \{0, 1\}$, the proof splits according to the following complementary cases:

$\mathsf{OPT}_\mathsf{B}(\Pi_0) < 1$ **and** $\mathsf{OPT}_\mathsf{B}(\Pi_1) < 1$. The induction hypothesis yields that $\mathsf{OPT}_\mathsf{A}(\Pi_0) = 1$ and $\mathsf{OPT}_\mathsf{A}(\Pi_1) = 1$. Proposition 3.8 now yields that $\mathsf{OPT}_\mathsf{B}(\Pi) < 1$ and $\mathsf{OPT}_\mathsf{A}(\Pi) = 1$, regardless of the party controlling $\mathsf{root}(\Pi)$.

$\mathsf{OPT}_\mathsf{B}(\Pi_0) = 1$ **and** $\mathsf{OPT}_\mathsf{B}(\Pi_1) = 1$. The induction hypothesis yields that $\mathsf{OPT}_\mathsf{A}(\Pi_0) < 1$ and $\mathsf{OPT}_\mathsf{A}(\Pi_1) < 1$. Proposition 3.8 now yields that $\mathsf{OPT}_\mathsf{B}(\Pi) = 1$ and $\mathsf{OPT}_\mathsf{A}(\Pi) < 1$, regardless of the party controlling $\mathsf{root}(\Pi)$.

$\mathsf{OPT}_\mathsf{B}(\Pi_0) = 1$ **and** $\mathsf{OPT}_\mathsf{B}(\Pi_1) < 1$. The induction hypothesis yields that $\mathsf{OPT}_\mathsf{A}(\Pi_0) < 1$ and $\mathsf{OPT}_\mathsf{A}(\Pi_1) = 1$. If A controls $\mathsf{root}(\Pi)$, Proposition 3.8 yields that $\mathsf{OPT}_\mathsf{A}(\Pi) = 1$ and $\mathsf{OPT}_\mathsf{B}(\Pi) < 1$. If B controls $\mathsf{root}(\Pi)$, Proposition 3.8 yields that $\mathsf{OPT}_\mathsf{A}(\Pi) < 1$ and $\mathsf{OPT}_\mathsf{B}(\Pi) = 1$. Hence, the proof follows.

$\mathsf{OPT}_\mathsf{B}(\Pi_0) < 1$ **and** $\mathsf{OPT}_\mathsf{B}(\Pi_1) = 1$. The proof follows arguments similar to the previous case. □

In the next sections, we show the connection between the optimal valid attack and recursive biased-continuation attacks, by connecting them both to a specific measure over the protocol's leaves, called here the "dominated measure" of a protocol.

[23] Recall that for a (possible partial) transcript u, Π_u is the protocol Π, conditioned that $u_1, \ldots, u_{|u|}$ were the first $|u|$ messages.

[24] Recall that λ is the string representation of the root of $\mathcal{T}(\Pi)$.

3.3 Dominated Measures

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{OPT}_\mathsf{A}(\Pi) = 1$ (and thus, by Proposition 3.8, $\mathsf{OPT}_\mathsf{B}(\Pi) < 1$). In such a protocol, the optimal attacker for A always has a winning strategy, regardless of B's strategy (honest or not). Our goal is to define a measure $M_\Pi^\mathsf{A} : \mathcal{L}(\Pi) \to [0,1]$ that will capture the "$1 - \mathsf{OPT}_\mathsf{B}(\Pi)$" advantage that party A has over party B. Specifically, we would like that $\mathrm{E}_{\langle \Pi \rangle}[M_\Pi^\mathsf{A}] = 1 - \mathsf{OPT}_\mathsf{B}(\Pi)$.

Recall that $\mathsf{OPT}_\mathsf{B}(\Pi)$ is the expected outcome of the protocol $(\mathsf{A}, \mathsf{B}')$, where B' is the optimal attacker for B. To achieve our goal, M_Π^A must "behave" similarly to the expected outcome of $(\mathsf{A}, \mathsf{B}')$. Naturally, such measure will be defined recursively. On A-controlled nodes, its expected value (over a choice of a random leaf in the original protocol Π) should be the weighted average of the expected values of the lower-level measures—similarly to the expected outcome of $(\mathsf{A}, \mathsf{B}')$, which is the weighted average of the expected outcomes of the subprotocols. On B-controlled nodes, the situation is trickier. B' chooses to send the message that minimizes the expected outcome of $(\mathsf{A}, \mathsf{B}')$. Assuming that the lower-level measures already behave like the expected outcome of $(\mathsf{A}, \mathsf{B}')$, B' actually chooses the message for which the expected value of the lower-level measure is smaller. But the expected value of M_Π^A remains the weighted average of the expected values of the lower-level measures. To fix this, we lower the value of the lower-level measure whose expected outcome is larger, so that the expected value of both lower-level measures is equal. The above discussion leads to the following measure over the protocol's leaves.

Definition 3.10 (Dominated Measures). The A-dominated measure of protocol $\Pi = (\mathsf{A}, \mathsf{B})$, denoted M_Π^A, is a measure over $\mathcal{L}(\Pi)$ defined by $M_\Pi^\mathsf{A}(\ell) = \chi_\Pi(\ell)$ if $\mathsf{round}(\Pi) = 0$, and otherwise recursively defined by

$$M_\Pi^\mathsf{A}(\ell) = \begin{cases} 0, & e_\Pi(\lambda, \ell_1) = 0;\text{[25]} \\ M_{\Pi_{\ell_1}}^\mathsf{A}(\ell_{2,\ldots,|\ell|}), & e_\Pi(\lambda, \ell_1) = 1; \\ M_{\Pi_{\ell_1}}^\mathsf{A}(\ell_{2,\ldots,|\ell|}), & e_\Pi(\lambda, \ell_1) \notin \{0,1\} \\ & \wedge (\mathsf{A} \text{ controls } \mathsf{root}(\Pi) \vee \mathsf{Smaller}_\Pi(\ell_1)); \\ \dfrac{\mathrm{E}_{\langle \Pi_{1-\ell_1} \rangle}\left[M_{\Pi_{1-\ell_1}}^\mathsf{A}\right]}{\mathrm{E}_{\langle \Pi_{\ell_1} \rangle}\left[M_{\Pi_{\ell_1}}^\mathsf{A}\right]} \cdot M_{\Pi_{\ell_1}}^\mathsf{A}(\ell_{2,\ldots,|\ell|}), & \text{otherwise,} \end{cases}$$

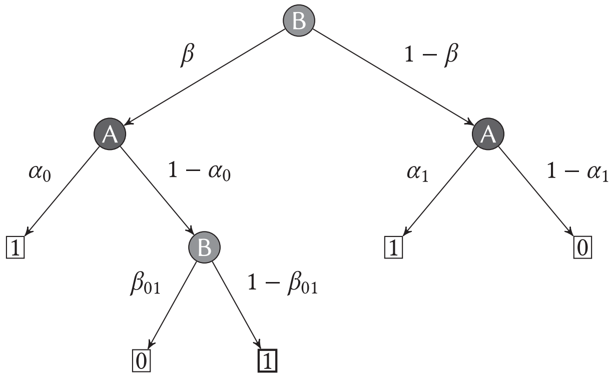
where $\mathsf{Smaller}_\Pi(\ell_1) = 1$ if $\mathrm{E}_{\langle \Pi_{\ell_1} \rangle}[M_{\Pi_{\ell_1}}^\mathsf{A}] \leq \mathrm{E}_{\langle \Pi_{1-\ell_1} \rangle}[M_{\Pi_{1-\ell_1}}^\mathsf{A}]$. Finally, we let $M_\perp^\mathsf{A}$ be the zero measure.

The B-dominated measure of protocol Π, denoted M_Π^B, is analogously defined, except that $M_\Pi^\mathsf{B}(\ell) = 1 - \chi_\Pi(\ell)$ if $\mathsf{round}(\Pi) = 0$.

*Example 3.11 (*A*-dominated Measure).* Before continuing with the formal proof, we believe the reader might find the following concrete example useful. Let $\Pi = (\mathsf{A}, \mathsf{B})$ be the protocol described in Figure 2(a) and assume for the sake of this example that $\alpha_0 < \alpha_1$. The A-dominated measures of Π and its subprotocols are given in Figure 2(b).

We would like to highlight some points regarding the calculations of the A-dominated measures. The first point we note is that $M_{\Pi_{011}}^\mathsf{A}(011) = 1$ but $M_{\Pi_{01}}^\mathsf{A}(011) = 0$. Namely, the A-dominated measure of the subprotocol Π_{011} assigns the leaf represented by the string 011 with the value 1, while the A-dominated measure of the subprotocol Π_{01} (for which Π_{011} is a subprotocol) assigns the same leaf with the value 0. This follows since $\mathrm{E}_{\langle \Pi_{010} \rangle}[M_{\Pi_{010}}^\mathsf{A}] = 0$ and $\mathrm{E}_{\langle \Pi_{011} \rangle}[M_{\Pi_{011}}^\mathsf{A}] = 1$, which yield that $\mathsf{Smaller}_{\Pi_{01}}(1) = 0$ (recall that $\mathsf{Smaller}_{\Pi'}(b) = 0$ if and only if the expected value of the A-dominated measure of Π'_b is larger than that of the A-dominated measure of Π'_{1-b}). Hence, Definition 3.10 with

[25] Recall that for transcript ℓ, ℓ_1 stands for the first messages sent in ℓ.



(a) Protocol $\Pi = (\mathsf{A}, \mathsf{B})$. The label of an internal node denotes the name of the party controlling it, and that of a leaf denotes its value. The label on an edge leaving a node u to node u' denotes the probability that a random execution of Π visits u' once in u. Finally, all nodes are represented as strings from the root of Π, even when considering subprotocols (e.g., the string representations of the leaf with the thick borders is 011).

	Leaves				
Measures	00	010	011	10	11
$M^{\mathsf{A}}_{\Pi_{00}}$	1				
$M^{\mathsf{A}}_{\Pi_{010}}$		0			
$M^{\mathsf{A}}_{\Pi_{011}}$			1		
$M^{\mathsf{A}}_{\Pi_{01}}$		0	0		
$M^{\mathsf{A}}_{\Pi_{0}}$	1	0	0		
$M^{\mathsf{A}}_{\Pi_{10}}$				1	
$M^{\mathsf{A}}_{\Pi_{11}}$					0
$M^{\mathsf{A}}_{\Pi_{1}}$				1	0
M^{A}_{Π}	1	0	0	α_0/α_1	0

(b) Calculating the A-dominated measure of Π. The A-dominated measure of a subprotocol Π_u, is only defined over the leaves in the subtree $\mathcal{T}(\Pi_u)$.

Fig. 2. An example of a (coin-flipping) protocol is given in (a), and an example of how to calculate its A-dominated measure is given in (b).

respect to Π_{01} now yields that

$$\begin{aligned} M^{\mathsf{A}}_{\Pi_{01}}(011) &= \frac{\mathrm{E}_{\langle \Pi_{010} \rangle}\left[M^{\mathsf{A}}_{\Pi_{010}}\right]}{\mathrm{E}_{\langle \Pi_{011} \rangle}\left[M^{\mathsf{A}}_{\Pi_{011}}\right]} \cdot M^{\mathsf{A}}_{\Pi_{011}}(011) \\ &= \frac{0}{1} \cdot 1 = 0. \end{aligned}$$

The second point we note is that $M^{\mathsf{A}}_{\Pi_1}(10) = 1$ but $M^{\mathsf{A}}_{\Pi}(10) = \frac{\alpha_0}{\alpha_1}$ (recall that we assumed that $\alpha_0 < \alpha_1$, so $\frac{\alpha_0}{\alpha_1} < 1$). This follows similar arguments to the previous point; it holds that $\mathrm{E}_{\langle \Pi_0 \rangle}[M^{\mathsf{A}}_{\Pi_0}] = \alpha_0$ and $\mathrm{E}_{\langle \Pi_1 \rangle}[M^{\mathsf{A}}_{\Pi_1}] = \alpha_1$, which yield that $\mathsf{Smaller}_{\Pi}(1) = 0$ (since $\alpha_0 < \alpha_1$). Definition 3.10 with respect to Π now yields that

$$\begin{aligned} M_\Pi^{\mathsf{A}}(10) &= \frac{\mathrm{E}_{\langle \Pi_0 \rangle}\left[M_{\Pi_0}^{\mathsf{A}}\right]}{\mathrm{E}_{\langle \Pi_1 \rangle}\left[M_{\Pi_1}^{\mathsf{A}}\right]} \cdot M_{\Pi_1}^{\mathsf{A}}(10) \\ &= \frac{\alpha_0}{\alpha_1} \cdot 1 = \frac{\alpha_0}{\alpha_1}. \end{aligned}$$

The third and final point we note is that $\mathrm{E}_{\langle \Pi \rangle}[M_\Pi^{\mathsf{A}}] = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi)$. By the assumption that $\alpha_0 < \alpha_1$, it holds that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \alpha_0$. Independently, let us calculate the expected value of the A-dominated measure. Since $\mathrm{Supp}(M_\Pi^{\mathsf{A}}) = \{00, 01\}$, it holds that

$$\begin{aligned} \mathrm{E}_{\langle \Pi \rangle}\left[M_\Pi^{\mathsf{A}}\right] &= \mathrm{v}_\Pi(00) \cdot M_\Pi^{\mathsf{A}}(00) + \mathrm{v}_\Pi(10) \cdot M_\Pi^{\mathsf{A}}(10) \\ &= \beta \cdot \alpha_0 \cdot 1 + (1-\beta) \cdot \alpha_1 \cdot \frac{\alpha_0}{\alpha_1} \\ &= \alpha_0. \end{aligned}$$

Hence, $\mathrm{E}_{\langle \Pi \rangle}[M_\Pi^{\mathsf{A}}] = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi)$.

Note that the A-dominated measure is B-*immune*—if B controls a node u, the expected value of the measure is that of the lowest measure of the subprotocols Π_{u0} and Π_{u1}, whereas if A controls a node u, the expected value of the A-dominated measure is the weighted average of the measures of the same subprotocols (according to the edge distribution). In both cases, the A-dominated measure indeed "captures" the behavior of the optimal attacker for B. This observation is formally stated as the following lemma:

Lemma 3.12. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol and let* M_Π^{A} *be its* A*-dominated measure. Then* $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1 - \mathrm{E}_{\langle \Pi \rangle}[M_\Pi^{\mathsf{A}}]$.

In particular, since $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ if and only if $\mathsf{OPT}_{\mathsf{B}}(\Pi) < 1$ (Proposition 3.8), it holds that $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ if and only if $\mathrm{E}_{\langle \Pi \rangle}[M_\Pi^{\mathsf{A}}] > 0$.

Toward proving Lemma 3.12, we first note that the definition of M_Π^{A} ensures three important properties.

Proposition 3.13. *Let* Π *be a protocol with* $\mathrm{e}_\Pi(\lambda, b) \notin \{0,1\}$ *for both* $b \in \{0,1\}$. *Then*

(1) (A-*maximal)* A *controls* $\mathsf{root}(\Pi) \Rightarrow (M_\Pi^{\mathsf{A}})_b \equiv M_{\Pi_b}^{\mathsf{A}}$ *for both* $b \in \{0,1\}$.[26]

(2) (B-*minimal)* B *controls* $\mathsf{root}(\Pi) \Rightarrow$

$$\left(M_\Pi^{\mathsf{A}}\right)_b \equiv \begin{cases} M_{\Pi_b}^{\mathsf{A}}, & \mathsf{Smaller}_\Pi(b) = 1; \\ \frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M_{\Pi_{1-b}}^{\mathsf{A}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M_{\Pi_b}^{\mathsf{A}}\right]} \cdot M_{\Pi_b}^{\mathsf{A}}, & \textit{otherwise}. \end{cases}$$

(3) (B-*immune)* B *controls* $\mathsf{root}(\Pi) \Rightarrow \mathrm{E}_{\langle \Pi_0 \rangle}[(M_\Pi^{\mathsf{A}})_0] = \mathrm{E}_{\langle \Pi_1 \rangle}[(M_\Pi^{\mathsf{A}})_1]$.

Namely, if A controls $\mathsf{root}(\Pi)$, the A-*maximal* property of M_Π^{A} (the A-dominated measure of Π) ensures that the restrictions of this measure to the subprotocols of Π are the A-dominated measures of these subprotocols. In the complementary case, i.e., B controls $\mathsf{root}(\Pi)$, the B-*minimal* property of M_Π^{A} ensures that for at least one subprotocol of Π, the restriction of this measure to this subprotocol is equal to the A-dominated measure of the subprotocol. Finally, the B-*immune*

[26] Recall that for a measure $M : \mathcal{L}(\Pi) \to [0,1]$ and a bit b, $(M)_b$ is the measure induced by M when restricted to $\mathcal{L}(\Pi_b) \subseteq \mathcal{L}(\Pi)$.

property of M^{A}_{Π} ensures that the expected values of the measures derived by restricting M^{A}_{Π} to the subprotocols of Π are equal (and hence, they are also equal to the expected value of M^{A}_{Π}).

Proof of Proposition 3.13. The proof of Items 1 and 2 (A-maximal and B-minimal) immediately follows from Definition 3.10.

Toward proving Item 3 (B-immune), we will assume that B controls $\operatorname{root}(\Pi)$. If $\mathsf{Smaller}_{\Pi}(0) = \mathsf{Smaller}_{\Pi}(1) = 1$, the proof again follows immediately from Definition 3.10. In the complementary case, i.e., $\mathsf{Smaller}_{\Pi}(b) = 0$ and $\mathsf{Smaller}_{\Pi}(1-b) = 1$ for some $b \in \{0,1\}$, it holds that

$$\begin{aligned} \mathrm{E}_{\langle \Pi_b \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_b\right] &= \mathrm{E}_{\langle \Pi_b \rangle}\left[\frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M^{\mathsf{A}}_{\Pi_{1-b}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M^{\mathsf{A}}_{\Pi_b}\right]} \cdot M^{\mathsf{A}}_{\Pi_b}\right] \\ &= \frac{\mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M^{\mathsf{A}}_{\Pi_{1-b}}\right]}{\mathrm{E}_{\langle \Pi_b \rangle}\left[M^{\mathsf{A}}_{\Pi_b}\right]} \cdot \mathrm{E}_{\langle \Pi_b \rangle}\left[M^{\mathsf{A}}_{\Pi_b}\right] \\ &= \mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[M^{\mathsf{A}}_{\Pi_{1-b}}\right] \\ &= \mathrm{E}_{\langle \Pi_{1-b} \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_{1-b}\right], \end{aligned}$$

where the first and last equalities follow from the B-minimal property of M^{A}_{Π} (Item 2). □

We are now ready to prove Lemma 3.12.

Proof of Lemma 3.12. The proof is by induction on the round complexity of Π.

Assume that $\operatorname{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. If $\chi_{\Pi}(\ell) = 1$, then by Definition 3.10, it holds that $M^{\mathsf{A}}_{\Pi}(\ell) = 1$, implying that $\mathrm{E}_{\langle \Pi \rangle}[M^{\mathsf{A}}_{\Pi}] = 1$. The proof follows since in this case, by Proposition 3.9, $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 0$. In the complementary case, i.e., $\chi(\ell) = 0$, by Definition 3.10, it holds that $M^{\mathsf{A}}_{\Pi}(\ell) = 0$, implying that $\mathrm{E}_{\langle \Pi \rangle}[M^{\mathsf{A}}_{\Pi}] = 0$. The proof follows since in this case, by Proposition 3.9, $\mathsf{OPT}_{\mathsf{B}}(\Pi) = 1$.

Assume that the lemma holds for m-round protocols and that $\operatorname{round}(\Pi) = m+1$. For $b \in \{0,1\}$, let $\alpha_b := \mathrm{E}_{\langle \Pi_b \rangle}[M^{\mathsf{A}}_{\Pi_b}]$. The induction hypothesis yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi_b) = 1 - \alpha_b$ for both $b \in \{0,1\}$. If $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0,1\}$ (which also means that $e_{\Pi}(\lambda, 1-b) = 0$), the proof follows since Proposition 3.8 yields that $\mathsf{OPT}_{\mathsf{B}}(\Pi) = \mathsf{OPT}_{\mathsf{B}}(\Pi_b) = 1 - \alpha_b$, where Definition 3.10 yields that $\mathrm{E}_{\langle \Pi \rangle}[M^{\mathsf{A}}_{\Pi}] = \mathrm{E}_{\langle \Pi_b \rangle}[M^{\mathsf{A}}_{\Pi_b}] = \alpha_b$.

Assume $e_{\Pi}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$ and let $p := e_{\Pi}(\lambda, 0)$. The proof splits according to who controls the root of Π.

A **controls** $\operatorname{root}(\Pi)$. Definition 3.10 yields that

$$\begin{aligned} \mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &= p \cdot \mathrm{E}_{\langle \Pi_0 \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \\ &= p \cdot \mathrm{E}_{\langle \Pi_0 \rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] + (1-p) \cdot \mathrm{E}_{\langle \Pi_1 \rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right] \\ &= p \cdot \alpha_0 + (1-p) \cdot \alpha_1, \end{aligned}$$

where the second equality follows from the A-maximal property of $M^{\mathsf{A}}_{\Pi_b}$ (Proposition 3.13(1)). Using Proposition 3.8, we conclude that

$$\begin{aligned} \mathsf{OPT}_{\mathsf{B}}(\Pi) &= p \cdot \mathsf{OPT}_{\mathsf{B}}(\Pi_0) + (1-p) \cdot \mathsf{OPT}_{\mathsf{B}}(\Pi_1) \\ &= p \cdot (1 - \alpha_0) + (1-p) \cdot (1 - \alpha_1) \\ &= 1 - (p \cdot \alpha_0 + (1-p) \cdot \alpha_1) \\ &= 1 - \mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi}\right]. \end{aligned}$$

B **controls** root(Π). We assume that $\alpha_0 \leq \alpha_1$ (the complementary case is analogous). Proposition 3.8 and the induction hypothesis yield that $\mathsf{OPT}_\mathsf{B}(\mathsf{A},\mathsf{B}) = 1 - \alpha_0$. Hence, it is left to show that $\mathrm{E}_{\langle\Pi\rangle}[M_\Pi^\mathsf{A}] = \alpha_0$. The assumption that $\alpha_0 \leq \alpha_1$ yields that $\mathsf{Smaller}_\Pi(0) = 1$. Thus, by the B-minimal property of M_Π^A (Proposition 3.13(2)), it holds that $(M_\Pi^\mathsf{A})_0 \equiv M_{\Pi_0}^\mathsf{A}$. It follows that $\mathrm{E}_{\langle\Pi_0\rangle}[(M_\Pi^\mathsf{A})_0] = \alpha_0$, and the B-immune property of M_Π^A (Proposition 3.13(3)) yields that $\mathrm{E}_{\langle\Pi_1\rangle}[(M_\Pi^\mathsf{A})_1] = \alpha_0$. To conclude the proof, we compute

$$\begin{aligned}\mathrm{E}_{\langle\Pi\rangle}\left[M_\Pi^\mathsf{A}\right] &= p\cdot\mathrm{E}_{\langle\Pi_0\rangle}\left[\left(M_\Pi^\mathsf{A}\right)_0\right] + (1-p)\cdot\mathrm{E}_{\langle\Pi_1\rangle}\left[\left(M_\Pi^\mathsf{A}\right)_1\right]\\ &= p\cdot\alpha_0 + (1-p)\cdot\alpha_0\\ &= \alpha_0.\end{aligned}$$

□

Lemma 3.12 connects the success of the optimal attack to the expected value of the dominated measure. In the next section, we analyze the success of the recursive biased-continuation attack using this expected value. Unfortunately, this analysis does not seem to suffice for our goal. In Section 3.5, we generalize the dominated measure described above to a sequence of (alternating) dominated measures, where in Section 3.6 we use this new notion to prove that the recursive biased continuation is indeed a good attack.

3.4 Warmup—Proof Attempt Using a (Single) Dominated Measure

As mentioned above, the approach described in this section falls too short to serve our goals. Yet we describe it here as a detailed overview for the more complicated proof, given in the following sections (with respect to a sequence of dominated measures). Specifically, we sketch a proof of the following lemma, which relates the performance of the recursive biased-continuation attacker playing the role of A to the performance of the optimal (valid) attacker playing the role of B. The proof (see below) is via the A-dominated measure of Π defined above.[27]

Lemma 3.14. *Let* $\Pi = (\mathsf{A},\mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) > 0$, *let* $k \in \mathbb{N}$, *and let* $\mathsf{A}^{(k)}$ *be according to Algorithm 3.2. Then*

$$\mathsf{val}(\mathsf{A}^{(k)},\mathsf{B}) \geq \frac{1 - \mathsf{OPT}_\mathsf{B}(\Pi)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}.$$

The proof of the above lemma is a direct implication of the next lemma.

Lemma 3.15. *Let* $\Pi = (\mathsf{A},\mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) > 0$, *let* $k \in \mathbb{N}$, *and let* $\mathsf{A}^{(k)}$ *be according to Algorithm 3.2. Then*

$$\mathrm{E}_{\langle\mathsf{A}^{(k)},\mathsf{B}\rangle}\left[M_\Pi^\mathsf{A}\right] \geq \frac{\mathrm{E}_{\langle\Pi\rangle}\left[M_\Pi^\mathsf{A}\right]}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}.$$

Proof of Lemma 3.14. Immediately follows Lemmas 3.12 and 3.15 and Fact 2.7 (we can use Fact 2.7 since by Definition 3.10, $M_\Pi^\mathsf{A}(\ell) = 0$ for every $\ell \in \mathcal{L}_0(\Pi)$). □

We begin by sketching the proof of the following lemma, which is a special case of Lemma 3.15. Later we explain how to generalize the proof below to derive Lemma 3.15.

Lemma 3.16. *Let* $\Pi = (\mathsf{A},\mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) > 0$ *and let* $\mathsf{A}^{(1)}$ *be according to Algorithm 3.2. Then* $\mathrm{E}_{\langle\mathsf{A}^{(1)},\mathsf{B}\rangle}[M_\Pi^\mathsf{A}] \geq \frac{\mathrm{E}_{\langle\Pi\rangle}[M_\Pi^\mathsf{A}]}{\mathsf{val}(\Pi)}$.

[27] The formal proof of Lemma 3.14 follows its stronger variant, Lemma 3.25, introduced in Section 3.6.

Proof sketch. The proof is by induction on the round complexity of Π. The base case (i.e., $\mathrm{round}(\Pi) = 0$) is straightforward. Assume that the lemma holds for m-round protocols and that $\mathrm{round}(\Pi) = m + 1$. For $b \in \{0,1\}$, let $\alpha_b := \mathrm{E}_{\langle \Pi_b \rangle}[M^{\mathsf{A}}_{\Pi_b}]$ and let $p := e_\Pi(\lambda, 0)$.

If $\mathrm{root}(\Pi)$ is controlled by A, the A-maximal property of M^{A}_{Π} (Proposition 3.13(1)) yields that $\mathrm{E}_{\langle \Pi \rangle}[M^{\mathsf{A}}_{\Pi}] = p \cdot \alpha_0 + (1-p) \cdot \alpha_1$. It holds that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &= e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0) \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_0 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1) \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_1 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \\ &= p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_0 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_1 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right], \end{aligned} \tag{9}$$

where the second equality follows from Claim 3.4. Since $\mathsf{A}^{(1)}$ is stateless (Proposition 3.5), we can write Equation (9) as

$$\mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right]. \tag{10}$$

The A-maximal property of M^{A}_{Π} and Equation (10) yield that

$$\mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] = p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right]. \tag{11}$$

Applying the induction hypothesis on the right-hand side of Equation (11) yields that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &\geq p \cdot \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \cdot \frac{\alpha_0}{\mathsf{val}(\Pi_0)} + (1-p) \cdot \frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)} \cdot \frac{\alpha_1}{\mathsf{val}(\Pi_1)} \\ &= \frac{p \cdot \alpha_0 + (1-p) \cdot \alpha_1}{\mathsf{val}(\Pi)} \\ &= \frac{\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi}\right]}{\mathsf{val}(\Pi)}, \end{aligned}$$

which concludes the proof for the case that A controls $\mathrm{root}(\Pi)$.

If $\mathrm{root}(\Pi)$ is controlled by B, and assuming that $\alpha_0 \leq \alpha_1$ (the complementary case is analogous), it holds that $\mathrm{Smaller}_\Pi(0) = 1$. Thus, by the B-minimal property of M^{A}_{Π} (Proposition 3.13(2)), it holds that $(M^{\mathsf{A}}_{\Pi})_0 \equiv M^{\mathsf{A}}_{\Pi_0}$ and $(M^{\mathsf{A}}_{\Pi})_1 \equiv \frac{\alpha_0}{\alpha_1} M^{\mathsf{A}}_{\Pi_1}$. Hence, the B-immune property of M^{A}_{Π} (Proposition 3.13(3)) yields that $\mathrm{E}_{\langle \Pi \rangle}[M^{\mathsf{A}}_{\Pi}] = \alpha_0$. In addition, since B controls $\mathrm{root}(\Pi)$, the distribution of the edges $(\lambda, 0)$ and $(\lambda, 1)$ has not changed. It holds that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[M^{\mathsf{A}}_{\Pi}\right] &= p \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_0 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\left\langle (\mathsf{A}^{(1)},\mathsf{B})_1 \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \\ &\overset{(1)}{=} p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[\left(M^{\mathsf{A}}_{\Pi}\right)_1\right] \\ &= p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] + (1-p) \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[\frac{\alpha_0}{\alpha_1} M^{\mathsf{A}}_{\Pi_1}\right] \\ &= p \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_0}, \mathsf{B}_{\Pi_0} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_0}\right] + (1-p) \cdot \frac{\alpha_0}{\alpha_1} \cdot \mathrm{E}_{\left\langle \mathsf{A}^{(1)}_{\Pi_1}, \mathsf{B}_{\Pi_1} \right\rangle}\left[M^{\mathsf{A}}_{\Pi_1}\right], \end{aligned} \tag{12}$$

where (1) follows since $\mathsf{A}^{(1)}$ is stateless (Proposition 3.5). Applying the induction hypothesis on the right-hand side of Equation (12) yields that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[M_\Pi^{\mathsf{A}}\right] &\geq p \cdot \frac{\alpha_0}{\mathsf{val}(\Pi_0)} + (1-p)\cdot\frac{\alpha_0}{\alpha_1}\cdot\frac{\alpha_1}{\mathsf{val}(\Pi_1)} \\ &= \alpha_0\left(\frac{p}{\mathsf{val}(\Pi_0)} + \frac{1-p}{\mathsf{val}(\Pi_1)}\right) \\ &\overset{(1)}{\geq} \frac{\mathrm{E}_{\langle\Pi\rangle}\left[M_\Pi^{\mathsf{A}}\right]}{\mathsf{val}(\Pi)}, \end{aligned}$$

which concludes the proof for the case that B controls $\mathsf{root}(\Pi)$, and where (1) holds since

$$\frac{p}{\mathsf{val}(\Pi_0)} + \frac{1-p}{\mathsf{val}(\Pi_1)} \geq \frac{1}{\mathsf{val}(\Pi)}. \tag{13}$$

□

The proof of Lemma 3.15 follows from similar arguments to those used above for proving Lemma 3.16.[28] Informally, we proved Lemma 3.16 by showing that $\mathsf{A}^{(1)}$ "assigns" more weight to the dominated measure than A does. A natural step is to consider $\mathsf{A}^{(2)}$ and to see if it assigns more weight to the dominated measure than $\mathsf{A}^{(1)}$ does. It turns out that one can turn this intuitive argument into a formal proof and prove Lemma 3.14 by repeating this procedure with respect to many recursive biased-continuation attacks.[29]

The shortcoming of Lemma 3.14. Given a protocol $\Pi = (\mathsf{A},\mathsf{B})$, we are interested in the minimal value of κ for which $\mathsf{A}^{(\kappa)}$ biases the value of the protocol toward one with probability of at least 0.9 (as a concrete example). Following Lemma 3.14, it suffices to find a value κ such that

$$\mathsf{val}(\mathsf{A}^{(\kappa)},\mathsf{B}) \geq \frac{1-\mathsf{OPT}_\mathsf{B}(\Pi)}{\prod_{i=0}^{\kappa-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} \geq 0.9. \tag{14}$$

Using worst-case analysis, it suffices to find κ such that $(1-\mathsf{OPT}_\mathsf{B}(\Pi))/(0.9)^\kappa \geq 0.9$, where the latter dictates that

$$\kappa \geq \frac{\log\left(\frac{1}{1-\mathsf{OPT}_\mathsf{B}(\Pi)}\right)}{\log\left(\frac{1}{0.9}\right)}. \tag{15}$$

Recall that our ultimate goal is to implement an *efficient* attack on any coin-flipping protocol under the mere assumption that one-way functions do not exist. Specifically, we would like to do so by giving an efficient version of the recursive biased-continuation attack. At the very least, due to the recursive nature of the attack, this requires the protocols $(\mathsf{A}^{(1)},\mathsf{B}),\ldots,(\mathsf{A}^{(\kappa-1)},\mathsf{B})$ to be efficient in comparison to the basic protocol. The latter efficiency restriction together with the recursive definition of $\mathsf{A}^{(\kappa)}$ dictates that κ (the number of recursion calls) be constant.

Unfortunately, Equation (15) reveals that if $\mathsf{OPT}_\mathsf{B}(\Pi) \in 1-o(1)$, we need to take $\kappa \in \omega(1)$, yielding an inefficient attack.

[28] The proof sketch given for Lemma 3.16 is almost a formal proof, lacking only consideration of the base case and the extreme cases in which $e_\Pi(\lambda, b) = 1$ for some $b \in \{0,1\}$.

[29] The main additional complication in the proof of Lemma 3.14 is that the simple argument used to derive Equation (13) is replaced with the more general argument, described in Lemma 2.20.

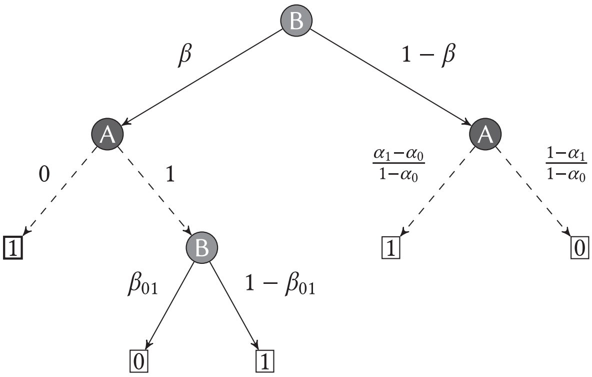

B
β
$1-\beta$
A
A
0
1
$\frac{\alpha_1-\alpha_0}{1-\alpha_0}$
$\frac{1-\alpha_1}{1-\alpha_0}$
1
B
1
0
β_{01}
$1-\beta_{01}$
0
1

Fig. 3. The conditional protocol $\Pi' = \Pi|\neg M_\Pi^{\mathsf{A}}$ of Π from Figure 2(a). Dashed edges are such that their distribution has changed. Note that due to this change, the leaf 00 (the leftmost leaf, marked by a thick border) is *inaccessible* in Π'. The B-dominated measure of Π' assigns a value of 1 to the leaf 010 and a value of 0 to all other leaves.

3.5 Back to the Proof—Sequence of Alternating Dominated Measures

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol and let M be a measure over the leaves of Π. Consider the variant of Π whose parties act identically to the parties in Π, but with the following tweak: when the execution reaches a leaf ℓ, the protocol restarts with probability $M(\ell)$. Namely, a random execution of the resulting (possibly inefficient) protocol is distributed like a random execution of Π, conditioned on not "hitting" the measure M.[30] The above is formally captured by the definition below.

3.5.1 Conditional Protocols.

Definition 3.17 (Conditional Protocols). Let Π be an m-round protocol and let M be a measure over $\mathcal{L}(\Pi)$ with $\mathrm{E}_{\langle\Pi\rangle}[M] < 1$. The m-round M-conditional protocol of Π, denoted $\Pi|\neg M$, is defined by the color function $\chi_{(\Pi|\neg M)} \equiv \chi_\Pi$, and the edge distribution function $e_{(\Pi|\neg M)}$ is defined by

$$e_{(\Pi|\neg M)}(u, ub) = \begin{cases} 0, & \mathrm{E}_{\langle\Pi_u\rangle}[M] = 1;\ ^{31} \\ e_\Pi(u, ub) \cdot \frac{1-\mathrm{E}_{\langle\Pi_{ub}\rangle}[M]}{1-\mathrm{E}_{\langle\Pi_u\rangle}[M]}, & \text{otherwise} \end{cases},$$

for every $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$ and $b \in \{0, 1\}$. The controlling scheme of the protocol $\Pi|\neg M$ is the same as in Π.

If $\mathrm{E}_{\langle\Pi\rangle}[M] = 1$ or $\Pi = \perp$, we set $\Pi|\neg M = \perp$.

Example 3.18 (Conditional Protocol). Once again we consider the protocol Π from Figure 2(a). In Figure 3, we present the conditional protocol $\Pi' = \Pi|\neg M_\Pi^{\mathsf{A}}$, namely, the protocol derived when protocol Π is conditioned not to "hit" the A-dominated measure of Π. We would like to highlight some points regarding this conditional protocol.

The first point we note is the changes in the edge distribution. Consider the root of Π_0 (i.e., the node 0). According to the calculations in Figure 2(b), it holds that $\mathrm{E}_{\langle\Pi_{00}\rangle}[M_\Pi^{\mathsf{A}}] = M_\Pi^{\mathsf{A}}(00) = 1$ and that $\mathrm{E}_{\langle\Pi_0\rangle}[M_\Pi^{\mathsf{A}}] = \alpha_0$. Hence, Definition 3.17 yields that

[30] For concreteness, one might like to consider the case where M is a set.

[31] Note that this case does not affect the resulting protocol, and is defined only to simplify future discussion.

$$\begin{aligned} e_{(\Pi|\neg M_\Pi^{\mathsf{A}})}(0,00) &= \alpha_0 \cdot \frac{1 - \mathrm{E}_{\langle \Pi_{00} \rangle}\left[M_\Pi^{\mathsf{A}}\right]}{1 - \mathrm{E}_{\langle \Pi_0 \rangle}\left[M_\Pi^{\mathsf{A}}\right]} \\ &= \alpha_0 \cdot \frac{0}{1-\alpha_0} \\ &= 0. \end{aligned}$$

Note that the above change makes the leaf 00 inaccessible in Π'. This occurs since $M_\Pi^{\mathsf{A}}(00) = 1$. Similar calculations yield the changes in the distribution of the edges leaving the root of Π_1 (i.e., the node 1).

The second point we note is that the conditional protocol is in fact a protocol. Namely, for every node, the sum of the probabilities of the edges leaving it is one. This is easily seen from Figure 3.

The third point we note is that the edge distribution of the root of Π does not change at all. This follows from Definition 3.17 and the fact that

$$\mathrm{E}_{\langle \Pi_0 \rangle}\left[M_\Pi^{\mathsf{A}}\right] = \mathrm{E}_{\langle \Pi_1 \rangle}\left[M_\Pi^{\mathsf{A}}\right] = \mathrm{E}_{\langle \Pi \rangle}\left[M_\Pi^{\mathsf{A}}\right] = \alpha_0.$$

The fourth point we note is that in the conditional protocol, an optimal valid attacker playing the role of B can bias the outcome toward zero with probability one. Namely, $\mathsf{OPT}_{\mathsf{B}}(\Pi|\neg M_\Pi^{\mathsf{A}}) = 1$. Such an attacker will send 0 as the first message, after which A must send 1 as the next message, and then the attacker will send 0. The outcome of this interaction is the value of the leaf 010, which is 0.

In the rest of the section, we show that the above observations can actually be generalized to statements regarding any conditional protocol.

The next proposition shows that the M-conditional protocol is indeed a protocol. It also shows a relation between the leaf distribution of the M-conditional protocol and the original protocol. Using this relation, we conclude that the set of possible transcripts of the M-conditional protocol is a subset of the original protocol's possible transcripts and that if M assigns a value of 1 to some transcript, then this transcript is inaccessible by the M-conditional protocol.

Proposition 3.19. *Let Π be a protocol and let M be a measure over $\mathcal{L}(\Pi)$ with $\mathrm{E}_{\langle \Pi \rangle}[M] < 1$. Then*

1. $\forall u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi):\ \mathsf{v}_{(\Pi|\neg M)}(u) > 0 \Rightarrow e_{(\Pi|\neg M)}(u, u0) + e_{(\Pi|\neg M)}(u, u1) = 1;$
2. $\forall \ell \in \mathcal{L}(\Pi):\ \mathsf{v}_{(\Pi|\neg M)}(\ell) = \mathsf{v}_\Pi(\ell) \cdot \frac{1-M(\ell)}{1-\mathrm{E}_{\langle \Pi \rangle}[M]};$
3. $\forall \ell \in \mathcal{L}(\Pi):\ \mathsf{v}_{(\Pi|\neg M)}(\ell) > 0 \Rightarrow \mathsf{v}_\Pi(\ell) > 0;$ *and*
4. $\forall \ell \in \mathcal{L}(\Pi):\ M(\ell) = 1 \Rightarrow \mathsf{v}_{(\Pi|\neg M)}(\ell) = 0.$

Proof. The first two items immediately follow from Definition 3.17. The last two items follow the second item. □

In addition to the above properties, Definition 3.17 guarantees the following "locality" property of the M-conditional protocol.

Proposition 3.20. *Let Π be a protocol and let M be a measure over $\mathcal{L}(\Pi)$. Then $(\Pi|\neg M)_u = \Pi_u|\neg(M)_u$ for every $u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$.*

Proof. Immediately follows from Definition 3.17. □

Proposition 3.20 helps us to apply induction on conditional protocols. Specifically, we use it to prove the following lemma, which relates the (dominated measure)-conditional protocol to the optimal (valid) attack.

Lemma 3.21. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol with $\mathsf{val}(\Pi) < 1$. Then $\mathsf{OPT}_{\mathsf{B}}(\Pi|\neg M_\Pi^{\mathsf{A}}) = 1$.*

This lemma justifies yet again the name of the A-dominated measure. Not only does this measure give a precise quantity to the advantage of the optimal attacker when taking the role of A over the one taking the role of B (Lemma 3.12), but also, when we condition on not "hitting" this measure, the optimal attacker taking the role of A no longer wins with probability one.

As an intuitive explanation, assume that $\mathsf{OPT}_\mathsf{A}(\Pi|\neg M_\Pi^\mathsf{A}) = 1$. By Proposition 3.9, it holds that $\mathsf{OPT}_\mathsf{B}(\Pi|\neg M_\Pi^\mathsf{A}) < 1$, and so there exists an A-dominated measure M in the conditional protocol $\Pi|\neg M_\Pi^\mathsf{A}$. Let the measure M' be the "union" of M_Π^A and M. It holds that M' (like M_Π^A itself) is A-maximal, B-minimal, and B-immune in Π, and that $\mathrm{E}_{\langle\Pi\rangle}[M'] > \mathrm{E}_{\langle\Pi\rangle}[M_\Pi^\mathsf{A}]$. Following similar arguments to those in the proof of Lemma 3.12, it also holds that $\mathrm{E}_{\langle\Pi\rangle}[M'] = 1 - \mathsf{OPT}_\mathsf{B}(\Pi)$. But Lemma 3.12 already showed that $1 - \mathsf{OPT}_\mathsf{B}(\Pi) = \mathrm{E}_{\langle\Pi\rangle}[M_\Pi^\mathsf{A}]$, a contradiction (in essence, Lemma 3.12 shows that M_Π^A is the "only" A-maximal, B-minimal, and B-immune measure in Π).

Proof of Lemma 3.21. First, we note that Fact 2.7 yields that $\mathrm{E}_{\langle\Pi\rangle}[M_\Pi^\mathsf{A}] \le \mathsf{val}(\Pi) < 1$, and hence $\Pi|\neg M_\Pi^\mathsf{A} \ne \perp$ (i.e., is a protocol). The rest of the proof is by induction on the round complexity of Π.

Assume that $\mathsf{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. Since it is assumed that $\mathsf{val}(\Pi) < 1$, it must be the case that $\chi_\Pi(\ell) = 0$. The proof follows since $M_\Pi^\mathsf{A}(\ell) = 0$, and thus $\Pi|\neg M_\Pi^\mathsf{A} = \Pi$, and since $\mathsf{OPT}_\mathsf{B}(\Pi) = 1$.

Assume the lemma holds for m-round protocols and that $\mathsf{round}(\Pi) = m + 1$. If $e_\Pi(\lambda, b) = 1$ for some $b \in \{0,1\}$, Definition 3.10 yields that $(M_\Pi^\mathsf{A})_b = M_{\Pi_b}^\mathsf{A}$. Moreover, Definition 3.17 yields that $e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda, b) = 1$. It holds that

$$\begin{aligned}\mathsf{OPT}_\mathsf{B}\left(\Pi|\neg M_\Pi^\mathsf{A}\right) &\overset{(1)}{=} \mathsf{OPT}_\mathsf{B}\left(\left(\Pi|\neg M_\Pi^\mathsf{A}\right)_b\right)\\ &\overset{(2)}{=} \mathsf{OPT}_\mathsf{B}\left(\Pi_b|\neg\left(M_\Pi^\mathsf{A}\right)_b\right)\\ &= \mathsf{OPT}_\mathsf{B}\left(\Pi_b|\neg M_{\Pi_b}^\mathsf{A}\right)\\ &\overset{(3)}{=} 1,\end{aligned} \tag{16}$$

where (1) follows from Proposition 3.8, (2) follows from Proposition 3.20, and (3) follows from the induction hypothesis.

In the complementary case, i.e., $e_\Pi(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$, the proof splits according to who controls the root of Π.

A *controls* $\mathsf{root}(\Pi)$. The assumption that $\mathsf{val}(\Pi) < 1$ dictates that $\mathsf{val}(\Pi_0) < 1$ or $\mathsf{val}(\Pi_1) < 1$. Consider the following complementary cases.

$\mathsf{val}(\Pi_0), \mathsf{val}(\Pi_1) < 1$: Proposition 3.8 yields that

$$\begin{aligned}&\mathsf{OPT}_\mathsf{B}\left(\Pi|\neg M_\Pi^\mathsf{A}\right)\\ &\overset{(1)}{=} e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,0)\cdot\mathsf{OPT}_\mathsf{B}\left(\left(\Pi|\neg M_\Pi^\mathsf{A}\right)_0\right) + e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,1)\cdot\mathsf{OPT}_\mathsf{B}\left(\left(\Pi|\neg M_\Pi^\mathsf{A}\right)_1\right)\\ &\overset{(2)}{=} e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,0)\cdot\mathsf{OPT}_\mathsf{B}\left(\Pi_0|\neg\left(M_\Pi^\mathsf{A}\right)_0\right) + e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,1)\cdot\mathsf{OPT}_\mathsf{B}\left(\Pi_1|\neg\left(M_\Pi^\mathsf{A}\right)_1\right)\\ &\overset{(3)}{=} e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,0)\cdot\mathsf{OPT}_\mathsf{B}\left(\Pi_0|\neg M_{\Pi_0}^\mathsf{A}\right) + e_{(\Pi|\neg M_\Pi^\mathsf{A})}(\lambda,1)\cdot\mathsf{OPT}_\mathsf{B}\left(\Pi_1|\neg M_{\Pi_1}^\mathsf{A}\right)\\ &\overset{(4)}{=} 1,\end{aligned}$$

where (1) follows from Proposition 3.8, (2) follows from Proposition 3.20, (3) follows from by the A-maximal property of M_Π^A (Proposition 3.13(1)), and (4) follows from the induction hypothesis.

$\mathsf{val}(\Pi_0) < 1$, $\mathsf{val}(\Pi_1) = 1$: By Definition 3.17, it holds that

$$\begin{aligned} e_{(\Pi|\neg M_\Pi^{\mathsf{A}})}(\lambda, 1) &= e_\Pi(\lambda, 1) \cdot \frac{1 - \mathrm{E}_{\langle \Pi_1 \rangle}\left[\left(M_\Pi^{\mathsf{A}}\right)_1\right]}{1 - \mathrm{E}_{\langle \Pi \rangle}\left[M_\Pi^{\mathsf{A}}\right]} \\ &\overset{(1)}{=} e_\Pi(\lambda, 1) \cdot \frac{1 - \mathrm{E}_{\langle \Pi_1 \rangle}\left[M_{\Pi_1}^{\mathsf{A}}\right]}{1 - \mathrm{E}_{\langle \Pi \rangle}\left[M_\Pi^{\mathsf{A}}\right]} \\ &\overset{(2)}{=} 0, \end{aligned}$$

where (1) follows from the A-maximal property of M_Π^{A} and (2) follows since $\mathsf{val}(\Pi_1) = 1$, which yields that $\mathrm{E}_{\langle \Pi_1 \rangle}[M_{\Pi_1}^{\mathsf{A}}] = 1$. Since $\Pi|\neg M_\Pi^{\mathsf{A}}$ is a protocol (Proposition 3.19), it holds that $e_{(\Pi|\neg M_\Pi^{\mathsf{A}})}(\lambda, 0) = 1$. The proof now follows from Equation (16).

$\mathsf{val}(\Pi_0) = 1$, $\mathsf{val}(\Pi_1) < 1$: The proof is analogous to the previous case.

B *controls* $\mathsf{root}(\Pi)$. Assume for simplicity that $\mathsf{Smaller}_\Pi(0) = 1$, namely, that $\mathrm{E}_{\langle \Pi_0 \rangle}[M_{\Pi_0}^{\mathsf{A}}] \le \mathrm{E}_{\langle \Pi_1 \rangle}[M_{\Pi_1}^{\mathsf{A}}]$ (the other case is analogous). It must hold that $\mathsf{val}(\Pi_0) < 1$ (otherwise, it holds that $\mathrm{E}_{\langle \Pi_0 \rangle}[M_{\Pi_0}^{\mathsf{A}}] = \mathrm{E}_{\langle \Pi_1 \rangle}[M_{\Pi_1}^{\mathsf{A}}] = 1$, which yields that $\mathsf{val}(\Pi_1) = 1$, and thus $\mathsf{val}(\Pi) = 1$). Hence, $\mathrm{E}_{\langle \Pi_0 \rangle}[M_{\Pi_0}^{\mathsf{A}}] < 1$, and Definition 3.17 yields that $e_{(\Pi|\neg M_\Pi^{\mathsf{A}})}(\lambda, 0) > 0$. By Proposition 3.8, it holds that

$$\begin{aligned} \mathsf{OPT}_{\mathsf{B}}\left(\Pi|\neg M_\Pi^{\mathsf{A}}\right) &\ge \mathsf{OPT}_{\mathsf{B}}\left(\left(\Pi|\neg M_\Pi^{\mathsf{A}}\right)_0\right) \\ &\overset{(1)}{=} \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg\left(M_\Pi^{\mathsf{A}}\right)_0\right) \\ &\overset{(2)}{=} \mathsf{OPT}_{\mathsf{B}}\left(\Pi_0|\neg M_{\Pi_0}^{\mathsf{A}}\right) \\ &\overset{(3)}{=} 1, \end{aligned}$$

where (1) follows from Proposition 3.20, (2) follows from the B-minimal property of M_Π^{A} (Proposition 3.13(2)), and (3) follows from the induction hypothesis. □

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol in which an optimal adversary playing the role of A biases the outcome toward one with probability one. Lemma 3.21 shows that in the conditional protocol $\Pi_{(\mathsf{B},0)} := \Pi|\neg M_\Pi^{\mathsf{A}}$, an optimal adversary playing the role of B can bias the outcome toward zero with probability one. Repeating this procedure with respect to $\Pi_{(\mathsf{B},0)}$ results in the protocol $\Pi_{(\mathsf{A},1)} := \Pi_{(\mathsf{B},0)}|\neg M_{\Pi_{(\mathsf{B},0)}}^{\mathsf{A}}$, in which again an optimal adversary playing the role of A can bias the outcome toward one with probability one. This procedure is stated formally in Definition 3.23.

3.5.2 Sequence of Dominated Measures.

Given a protocol (A, B), order the pairs $\{(\mathsf{C}, j)\}_{(\mathsf{C},j)\in\{\mathsf{A},\mathsf{B}\}\times\mathbb{N}}$ according to the sequence $(\mathsf{A}, 0), (\mathsf{B}, 0), (\mathsf{A}, 1), (\mathsf{B}, 1)$, and so on.

Notation 3.22. *Let* (A, B) *be a protocol. For* $j \in \mathbb{Z}$, *let* $\mathsf{pred}(\mathsf{A}, j) = (\mathsf{B}, j - 1)$ *and* $\mathsf{pred}(\mathsf{B}, j) = (\mathsf{A}, j)$, *and let* succ *be the inverse operation of* pred *(i.e.,* $\mathsf{succ}(\mathsf{pred}(\mathsf{C}, j)) = (\mathsf{C}, j)$*). For pairs* $(\mathsf{C}, j), (\mathsf{C}', j') \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{Z}$, *we write the following:*

- (C, j) *is* less than or equal to (C', j'), *denoted* $(\mathsf{C}, j) \preceq (\mathsf{C}', j')$, *if* $\exists\{(\mathsf{C}_1, j_1), \ldots, (\mathsf{C}_n, j_n)\}$ *such that* $(\mathsf{C}, j) = (\mathsf{C}_1, j_1)$, $(\mathsf{C}', j') = (\mathsf{C}_n, j_n)$, *and* $(\mathsf{C}_i, j_i) = \mathsf{pred}(\mathsf{C}_{i+1}, j_{i+1})$ *for any* $i \in [n - 1]$.
- (C, j) *is* less than (C', j'), *denoted* $(\mathsf{C}, j) \prec (\mathsf{C}', j')$, *if* $(\mathsf{C}, j) \preceq (\mathsf{C}', j')$ *and* $(\mathsf{C}, j) \ne (\mathsf{C}', j')$.

Finally, for $(\mathsf{C}, j) \succeq (\mathsf{A}, 0)$, *let* $[(\mathsf{C}, j)] := \{(\mathsf{C}', j') : (\mathsf{A}, 0) \preceq (\mathsf{C}', j') \preceq (\mathsf{C}, j)\}$.

Definition 3.23 (Dominated Measures Sequence). For a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ and $(\mathsf{C}, j) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$, the protocol $\Pi_{(\mathsf{C},j)}$ is defined by

$$\Pi_{(\mathsf{C},j)} = \begin{cases} \Pi, & (\mathsf{C}, j) = (\mathsf{A}, 0); \\ \Pi_{(\mathsf{C}',j')=\operatorname{pred}(\mathsf{C},j)}|\neg\left(M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}}\right), & \text{otherwise.}^{32} \end{cases}$$

Define the (C, j) dominated measures sequence of Π, denoted (C, j)-DMS(Π), by $\{M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}}\}_{(\mathsf{C}',j')\in[(\mathsf{C},j)]}$. Finally, for $z \in \mathbb{N}$, let $L^{\mathsf{C},z}_{\Pi} \equiv \sum_{j=0}^{z} M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}} \prod_{t=0}^{j-1}(1 - M^{\mathsf{C}}_{\Pi_{(\mathsf{C},t)}})$.

We show that $L^{\mathsf{A},z}_{\Pi}$ is a measure (i.e., its range is $[0, 1]$) and that its support is a subset of the 1-leaves of Π. We also give an explicit expression for its expected value (analogous to the expected value of M^{A}_{Π} given in Lemma 3.12).

Lemma 3.24. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol, let $z \in \mathbb{N}$, and let $L^{\mathsf{A},z}_{\Pi}$ be as in Definition 3.23. It holds that*

(1) $L^{\mathsf{A},z}_{\Pi}$ is a measure over $\mathcal{L}_1(\Pi)$:
 (a) $L^{\mathsf{A},z}_{\Pi}(\ell) \in [0, 1]$ for every $\ell \in \mathcal{L}(\Pi)$, and
 (b) $\operatorname{Supp}(L^{\mathsf{A},z}_{\Pi}) \subseteq \mathcal{L}_1(\Pi)$.
(2) $\mathrm{E}_{\langle\Pi\rangle}[L^{\mathsf{A},z}_{\Pi}] = \sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1 - \beta_t)(1 - \alpha_t)$, where $\alpha_j = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi_{(\mathsf{A},j)})$, $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}(\Pi_{(\mathsf{B},j)})$, and $\mathsf{OPT}_{\mathsf{A}}(\perp) = \mathsf{OPT}_{\mathsf{B}}(\perp) = 1$.

Proof. We prove the above two items separately.

Proof of Item 1. Let $\ell \in \mathcal{L}_0(\Pi)$. Since $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) = 0$ for every $j \in (z)$, it holds that $L^{\mathsf{A},z}_{\Pi}(\ell) = 0$.

Let $\ell \in \mathcal{L}_1(\Pi)$. Since $L^{\mathsf{A},z}_{\Pi}(\ell)$ is a sum of nonnegative numbers, it follows that its value is nonnegative. It is left to argue that $L^{\mathsf{A},z}_{\Pi}(\ell) \leq 1$. Since $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},z)}}$ is a measure, note that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},z)}}(\ell) \leq 1$. Thus,

$$\begin{aligned} L^{\mathsf{A},z}_{\Pi}(\ell) &= \sum_{j=0}^{z} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\ &\leq \prod_{t=0}^{z-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) + \sum_{j=0}^{z-1} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\ &= \left(\sum_{\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) + \sum_{j=0}^{z-1} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \left(\sum_{\mathcal{I}\subseteq(j-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\ &= \left(\sum_{\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) + \left(\sum_{\emptyset\neq\mathcal{I}\subseteq(z-1)} (-1)^{|\mathcal{I}|+1} \cdot \prod_{t\in\mathcal{I}} M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right) \\ &= 1. \end{aligned}$$

[32] Note that if $\mathrm{E}_{\langle\Pi_{(\mathsf{C},j)}\rangle}[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}] = 1$, Definition 3.17 yields that $\Pi_{\operatorname{succ}(\mathsf{C},j)} = \perp$. In fact, since we defined $\perp |\neg M = \perp$ for any measure M (also in Definition 3.17), it follows that $\Pi_{(\mathsf{C}',j')} = \perp$ for any $(\mathsf{C}', j') \succ (\mathsf{C}, j)$.

Proof of Item 2. By linearity of expectation, it suffices to prove that

$$\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}} \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}\right)\right] = \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t) \tag{17}$$

for any $j \in (z)$. Fix $j \in (z)$. If $\Pi_{(\mathsf{A},j)} = \perp$, then by Definition 3.10, it holds that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}$ is the zero measure, and both sides of Equation (17) equal 0.

In the following, we assume that $\Pi_{(\mathsf{A},j)} \neq \perp$. We first note that $\mathrm{E}_{\langle \Pi_{(\mathsf{C},t)} \rangle}[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},t)}}] < 1$ for any $(\mathsf{C},t) \in [\mathrm{pred}(\mathsf{A},j)]$ (otherwise, it must be that $\Pi_{(\mathsf{A},j)} = \perp$). Thus, Lemma 3.12 yields that $\alpha_t, \beta_t < 1$ for every $t \in (j-1)$. Hence, recursively applying Proposition 3.19(2) yields that

$$\mathrm{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) = \mathrm{v}_{\Pi}(\ell) \cdot \prod_{t=0}^{j-1} \frac{1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)}{1-\alpha_t} \cdot \frac{1 - M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)}{1-\beta_t} \tag{18}$$

for every $\ell \in \mathcal{L}(\Pi)$. Moreover, for $\ell \in \mathrm{Supp}(\Pi_{(\mathsf{A},j)})$, i.e., $\mathrm{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) > 0$, we can manipulate Equation (18) to get that

$$\mathrm{v}_{\Pi}(\ell) = \mathrm{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) \cdot \prod_{t=0}^{j-1} \frac{1-\alpha_t}{1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)} \cdot \frac{1-\beta_t}{1 - M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)} \tag{19}$$

for every $\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right)$.

It follows that

$$\begin{aligned}
&\mathrm{E}_{\langle \Pi \rangle}\left[M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}} \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}\right)\right] \\
&= \sum_{\ell \in \mathcal{L}(\Pi)} \mathrm{v}_{\Pi}(\ell) \cdot \left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right) \\
&\overset{(1)}{=} \sum_{\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right) \cap \mathcal{L}_1(\Pi)} \mathrm{v}_{\Pi}(\ell) \cdot \left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right) \\
&\overset{(2)}{=} \sum_{\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right) \cap \mathcal{L}_1(\Pi)} \mathrm{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) \cdot \prod_{t=0}^{j-1} \frac{1-\alpha_t}{1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)} \cdot \frac{1-\beta_t}{1 - M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell)} \\
&\quad \cdot \left(M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - M^{\mathsf{A}}_{\Pi_{(\mathsf{A},t)}}(\ell)\right)\right) \\
&\overset{(3)}{=} \sum_{\ell \in \mathrm{Supp}\left(\Pi_{(\mathsf{A},j)}\right) \cap \mathcal{L}_1(\Pi)} \mathrm{v}_{\left(\Pi_{(\mathsf{A},j)}\right)}(\ell) \cdot M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) \cdot \prod_{t=0}^{j-1}\left(1-\alpha_j\right)\left(1-\beta_j\right) \\
&= \alpha_j \cdot \prod_{t=0}^{j-1}(1-\beta_t)(1-\alpha_t),
\end{aligned}$$

concluding the proof. (1) follows since Definition 3.10 yields that $M^{\mathsf{A}}_{\Pi_{(\mathsf{A},j)}}(\ell) = 0$ for any $\ell \notin \mathrm{Supp}(\Pi_{(\mathsf{A},j)}) \cap \mathcal{L}_1(\Pi)$, (2) follows from Equation (19), and (3) follows since $M^{\mathsf{B}}_{\Pi_{(\mathsf{B},t)}}(\ell) = 0$ for every $\ell \in \mathcal{L}_1(\Pi)$ and $t \in (j-1)$. □

Using dominated measure sequences, we manage to give an improved bound for the success probability of the recursive biased-continuation attacks (compared to the bound of Lemma 3.16, which uses a single dominated measure). The improved analysis yields that a constant number of recursion calls of the biased-continuation attack is successful in biasing the protocol to an arbitrary constant close to either 0 or 1.

3.6 Improved Analysis Using Alternating Dominated Measures

We are finally ready to state two main lemmas, whose proofs—given in the next two sections—are the main technical contribution of Section 3, and then show how to use them to prove Theorem 3.3.

The first lemma is analogous to Lemma 3.14, but applied on the sequence of the dominated measures, and not just on a single dominated measure.

Lemma 3.25. *For a protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *with* $\mathsf{val}(\Pi) > 0$ *and* $z \in \mathbb{N}$*, it holds that*

$$\mathsf{val}(\mathsf{A}^{(k)}, \mathsf{B}) \geq \mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] \geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right]}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{j=0}^{z-1} \beta_j\right)^k$$

for every $k \in \mathbb{N}$*, where* $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}(\Pi_{(\mathsf{B},j)})$*, letting* $\mathsf{OPT}_{\mathsf{A}}(\perp) = 1$.

The above states that the recursive biased-continuation attacker biases the outcome of the protocol by a bound similar to that given in Lemma 3.14, but applied with respect to $L_{\Pi}^{\mathsf{A},z}$, instead of M_{Π}^{A} in Lemma 3.14. This is helpful since the expected value of $L_{\Pi}^{\mathsf{A},z}$ is strictly larger than that of M_{Π}^{A}. However, since $L_{\Pi}^{\mathsf{A},z}$ is defined with respect to a sequence of conditional protocols, we must "pay" the term $(1 - \sum_{j=0}^{z-1} \beta_j)^k$ in order to get this bound in the original protocol.

The following lemma states that Lemma 3.25 provides a sufficient bound. Specifically, it shows that if we take a long enough sequence of conditional protocols, the expected value of the measure $L_{\Pi}^{\mathsf{A},z}$ will be sufficiently large, while the payment term mentioned above will be kept sufficiently small.

Lemma 3.26. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol. Then for every* $c \in (0, \frac{1}{2}]$*, there exists* $z = z(c, \Pi) \in \mathbb{N}$ *(possibly exponential large) such that*

(1) $\mathrm{E}_{\langle \Pi \rangle}[L_{\Pi}^{\mathsf{A},z}] \geq c \cdot (1 - 2c)$ *and* $\sum_{j=0}^{z-1} \beta_j < c$*; or*
(2) $\mathrm{E}_{\langle \Pi \rangle}[L_{\Pi}^{\mathsf{B},z}] \geq c \cdot (1 - 2c)$ *and* $\sum_{j=0}^{z} \alpha_j < c$*,*

where $\alpha_j = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi_{(\mathsf{A},j)})$ *and* $\beta_j = 1 - \mathsf{OPT}_{\mathsf{A}}(\Pi_{(\mathsf{B},j)})$.

To derive Theorem 3.3, we take a sequence of the dominated measures that is long enough so that its accumulated weight will be sufficiently large. Furthermore, the weight of the dominated measures that precede the final dominated measure in the sequence is small (otherwise, we would have taken a shorter sequence), so the parties are "missing" these measures with high probability. The formal proof of Theorem 3.3 is given next, and the proofs of Lemmas 3.25 and 3.26 are given in Sections 3.7 and 3.8, respectively.

3.6.1 Proving Theorem 3.3.

Proof of Theorem 3.3. If $\mathsf{val}(\Pi) = 0$, Theorem 3.3 trivially holds. Assume that $\mathsf{val}(\Pi) > 0$, let z be the minimum integer guaranteed by Lemma 3.26 for $c = \varepsilon/2$, and let $\kappa = \lceil \frac{\log(\frac{2}{\varepsilon})}{\log(\frac{1-\varepsilon/2}{1-\varepsilon})} \rceil \in \widetilde{O}(1/\varepsilon)$.

If z satisfies Item 1 of Lemma 3.26, assume toward a contradiction that $\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) \leq 1 - \varepsilon$. Lemma 3.25 yields that

$$\begin{aligned}\mathsf{val}(\mathsf{A}^{(\kappa)}, \mathsf{B}) &\geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right]}{\prod_{i=0}^{\kappa-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{j=0}^{z-1} \beta_j\right)^{\kappa} \\ &> \frac{\varepsilon(1-\varepsilon)}{2} \cdot \left(\frac{1-\varepsilon/2}{1-\varepsilon}\right)^{\kappa} \\ &\geq 1 - \varepsilon,\end{aligned}$$

and a contradiction is derived.

If z satisfies Item 2 of Lemma 3.26, an analogous argument to the above yields that $\mathsf{val}(\mathsf{A}, \mathsf{B}^{(\kappa)}) \leq \varepsilon$. □

3.7 Proving Lemma 3.25

3.7.1 Outline. We would like to follow the proof's outline of Lemma 3.16, which is a special case of Lemma 3.25 for $k = 1$ and $z = 0$ (i.e., only a single dominated measure instead of a sequence).

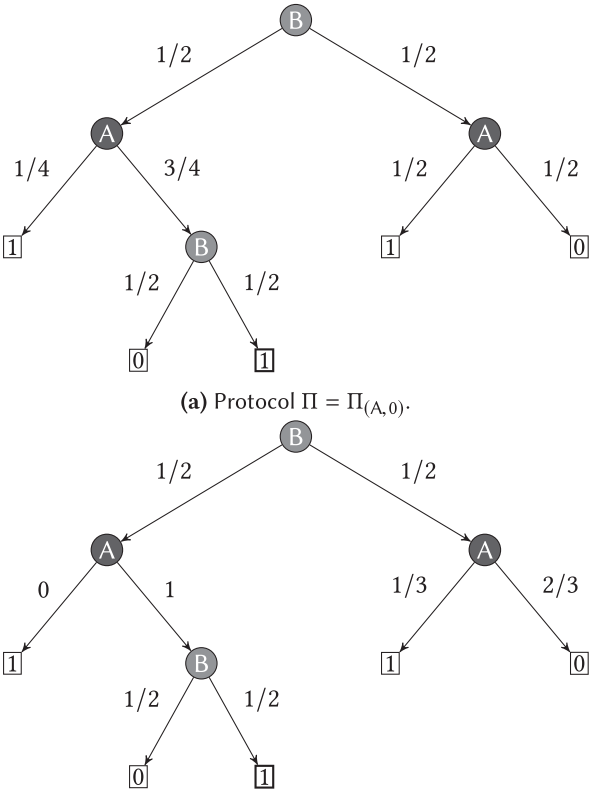
The proof of Lemma 3.16 was done through the following steps: (1) we applied the induction hypothesis to the subprotocols Π_0 and Π_1 with respect to their A-dominated measures, $M_{\Pi_0}^{\mathsf{A}}$ and $M_{\Pi_1}^{\mathsf{A}}$; (2) we related, using Proposition 3.13, $M_{\Pi_0}^{\mathsf{A}}$ and $M_{\Pi_1}^{\mathsf{A}}$ to $(M_{\Pi}^{\mathsf{A}})_0$ and $(M_{\Pi}^{\mathsf{A}})_1$, where the latter are the restrictions of the A-dominated measure of Π to Π_0 and Π_1; (3) if A controls the root, then we used the properties of $\mathsf{A}^{(1)}$ (specifically, the way it changes the edges' distribution) to complete the proof; and (4) if B controls the root, then we used a convexity-type argument to complete the proof.

Let's try to extend the above outline for a sequence of two dominated measures. It will be useful to consider a specific protocol, presented in Figure 4(a) (this protocol is an instantiation of the protocol we have been using thus far for the examples). Recall that the A-dominated measure of $\Pi = \Pi_{(\mathsf{A},0)}$ assigns $M_{\Pi}^{\mathsf{A}}(00) = 1$ (the leftmost leaf), $M_{\Pi}^{\mathsf{A}}(10) = 1/2$ (the second to the rightmost leaf), and zero to the rest of the leaves. Using M_{Π}^{A}, we can now compute $\Pi_{(\mathsf{B},0)}$, presented in Figure 4(b). Now, consider the sequence of two dominated measures for Π_1, presented in Figure 5(a). The A-dominated measure of $\Pi_1 = (\Pi_1)_{(\mathsf{A},0)}$ assigns $M_{\Pi_1}^{\mathsf{A}}(10) = 1$ and $M_{\Pi_1}^{\mathsf{A}}(11) = 0$, and using it, we can compute $(\Pi_1)_{(\mathsf{B},0)}$, presented in Figure 5(b).

The first step of the outline above is to apply the induction hypothesis to the subprotocol Π_1. When trying to extend this outline for proving Lemma 3.25, we face a problem, since $(\Pi_1)_{(\mathsf{B},0)}$ is not the same protocol as $(\Pi_{(\mathsf{B},0)})_1$. The latter is a consequence of the fact that $(M_{\Pi}^{\mathsf{A}})_1 \neq M_{\Pi_1}^{\mathsf{A}}$. In fact, we implicitly faced the same problem in the proof of Lemma 3.16, where we used Proposition 3.13 to show that $(M_{\Pi}^{\mathsf{A}})_1 = (1/2) \cdot M_{\Pi_1}^{\mathsf{A}}$, thus still enabling us to use the induction hypothesis. At this point, we observe that the proof of Lemma 3.16 can also be viewed differently. Instead of applying the induction hypothesis on $M_{\Pi_1}^{\mathsf{A}}$ and using Proposition 3.13, we can apply the induction hypothesis directly to the measure $(1/2) \cdot M_{\Pi_1}^{\mathsf{A}}$. This requires strengthening of the statement of the lemma to consider *submeasures* of dominated measures, namely, measures of the form $\eta \cdot M$, for $0 \leq \eta \leq 1$ and M being some dominated measure.

Using a sequence of dominated submeasures is the path we take for proving Lemma 3.25. The outline of the proof is as follows:

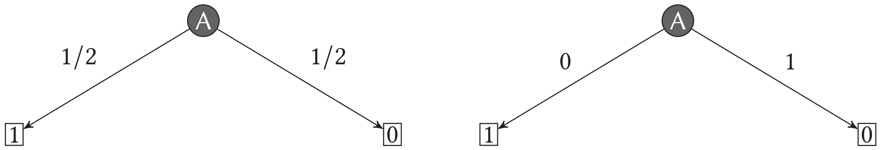
(1) Define the $(\Pi, \boldsymbol{\eta})$-dominated submeasures sequence, where $\boldsymbol{\eta}$ is a vector of real values in $[0, 1]$ (Definition 3.27).
(2) Extend the statement of Lemma 3.25 to handle dominated submeasures sequences (Lemma 3.28).



(a) Protocol $\Pi = \Pi_{(\mathrm{A},0)}$.

(b) Protocol $\Pi_{(\mathrm{B},0)}$.

Fig. 4. An example of a coin-flipping protocol to the left and its conditional protocol to the right, when conditioning not to "hit" the A-dominated measure.



(a) Protocol $\Pi_1 = (\Pi_1)_{(\mathrm{A},0)}$.

(b) Protocol $(\Pi_1)_{(\mathrm{B},0)}$.

Fig. 5. The subprotocol Π_1 of the protocol from Figure 4 and its conditional protocol.

(3) Given $\boldsymbol{\eta}$, carefully define $\boldsymbol{\eta}_0$ and $\boldsymbol{\eta}_1$ such that the restrictions of the $(\Pi, \boldsymbol{\eta})$-dominated submeasures sequence are exactly the measures used in the $(\Pi_0, \boldsymbol{\eta}_0)$-dominated submeasures sequence and in the $(\Pi_1, \boldsymbol{\eta}_1)$-dominated submeasure sequence (Definition 3.29 and Claim 3.30).
(4) Apply the induction hypothesis to the $(\Pi_0, \boldsymbol{\eta}_0)$-dominated submeasures sequence and the $(\Pi_1, \boldsymbol{\eta}_1)$-dominated submeasures sequence.
(5) If A controls the root, then use the properties of $\mathrm{A}^{(1)}$ to complete the proof.
(6) If B controls the root, then use a convexity-type argument to complete the proof.

The formal proof, given below, follows precisely this outline. Unlike in the proof of Lemma 3.16, the last two steps are not trivial, and require careful analysis.

3.7.2 *Formal Proof of Lemma 3.25.*

The proof of Lemma 3.25 is an easy implication of Lemma 3.24 and the following key lemma, defined with respect to sequences of *submeasures* of the dominated measure.

Definition 3.27 (Dominated Submeasures Sequence). For a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, a pair $(\mathsf{C}^*, j^*) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$, and $\boldsymbol{\eta} = \{\eta_{(\mathsf{C},j)} \in [0,1]\}_{(\mathsf{C},j) \in [(\mathsf{C}^*, j^*)]}$, define the protocol $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ by

$$\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)} := \begin{cases} \Pi, & (\mathsf{C},j) = (\mathsf{A},0); \\ \widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C}',j')=\mathsf{pred}(\mathsf{C},j)}|_{\neg\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')}\right)}, & \text{otherwise} \end{cases},$$

where $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')} \equiv \eta_{(\mathsf{C}',j')} \cdot M^{\mathsf{C}'}_{\Pi^{\boldsymbol{\eta}}_{(\mathsf{C}',j')}}$. For $(\mathsf{C},j) \in [(\mathsf{C}^*, j^*)]$, define the $(\mathsf{C}, j, \boldsymbol{\eta})$-dominated measure sequence of Π, denoted $(\mathsf{C}, j, \boldsymbol{\eta})$-DMS$(\Pi)$, as $\{\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C}',j')}\}_{(\mathsf{C}',j') \in [(\mathsf{C},j)]}$, and let $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)} = \mathrm{E}_{\langle \widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)} \rangle}[\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}]$.[33]

Finally, let $\widehat{L}^{\mathsf{C},\boldsymbol{\eta}}_{\Pi} \equiv \sum_{j:(\mathsf{C},j) \in [(\mathsf{C}^*,j^*)]} \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)} \cdot \prod_{t=0}^{j-1} (1 - \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},t)})$.

Lemma 3.28. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol with* $\mathsf{val}(\Pi) > 0$, *let* $z \in \mathbb{N}$, *and let* $\boldsymbol{\eta} = \{\eta_{(\mathsf{C},j)} \in [0,1]\}_{(\mathsf{C},j) \in [(\mathsf{A},z)]}$. *For* $j \in (z)$, *let* $\alpha_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$, *and for* $j \in (z-1)$, *let* $\beta_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}$. *Then*

$$\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[\widehat{L}^{\mathsf{A},\boldsymbol{\eta}}_{\Pi}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1} (1-\beta_t)^{k+1} (1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}$$

for any positive $k \in \mathbb{N}$.

The proof of Lemma 3.28 is given below, but we first use it to prove Lemma 3.25.

Proof of Lemma 3.25. Let $\eta_{(\mathsf{C},j)} = 1$ for every $(\mathsf{C},j) \in [(\mathsf{A},z)]$ and let $\boldsymbol{\eta} = \{\eta_{(\mathsf{C},j)}\}_{(\mathsf{C},j) \in [(\mathsf{A},z)]}$. It follows that $\widehat{L}^{\mathsf{A},\boldsymbol{\eta}}_{\Pi} \equiv L^{\mathsf{A},z}_{\Pi}$. Applying Lemma 3.28 yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1} (1-\beta_t)^{k+1} (1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}, \tag{20}$$

where $\alpha_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$ and $\beta_j = \widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}$. Multiplying the jth summand of the right-hand side of Equation (20) by $\prod_{t=j}^{z-1} (1-\beta_j)^k \leq 1$ yields that

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] &\geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1} (1-\beta_t)(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \prod_{t=0}^{z-1} (1-\beta_t)^k \qquad (21) \\ &\geq \frac{\sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1} (1-\beta_t)(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{t=0}^{z-1} \beta_t\right)^k, \end{aligned}$$

where the second inequality follows since $\beta_j \geq 0$ and $(1-x)(1-y) \geq 1-(x+y)$ for any $x, y \geq 0$. By Lemma 3.12 and the definition of $\boldsymbol{\eta}$, it follows that $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)} = 1 - \mathsf{OPT}_{\mathsf{B}}(\Pi_{(\mathsf{A},j)})$ and $\widehat{\mu}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)} = 1 - \mathsf{OPT}_{\mathsf{A}}(\Pi_{(\mathsf{B},j)})$. Hence, plugging Lemma 3.24 into Equation (21) yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B} \rangle}\left[L^{\mathsf{A},z}_{\Pi}\right] \geq \frac{\mathrm{E}_{\langle \Pi \rangle}\left[L^{\mathsf{A},z}_{\Pi}\right]}{\prod_{i=0}^{k-1} \mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})} \cdot \left(1 - \sum_{t=0}^{z-1} \beta_t\right)^k. \tag{22}$$

[33] Note that for $\boldsymbol{\eta} = (1, 1, 1, \ldots, 1)$, Definition 3.27 coincides with Definition 3.23.

Finally, the proof is concluded, since by Lemma 3.24 and Fact 2.7, it immediately follows that $\mathsf{val}(\mathsf{A}^{(k)}, \mathsf{B}) \geq \mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B}\rangle}[L_{\Pi}^{\mathsf{A},z}]$. □

3.7.3 *Proving Lemma 3.28.*

Proof of Theorem 3.28. In the following, we fix a protocol Π, real vector $\boldsymbol{\eta} = \{\eta_{(\mathsf{C},j)}\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$, and a positive integer k. We also assume for simplicity that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)}$ is not the undefined protocol, i.e., $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)} \neq \perp$.[34] The proof is by induction on the round complexity of Π.

Base case. Assume $\mathsf{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. For $j \in (z)$, Definition 3.27 yields that $\chi_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\ell) = \chi_{\Pi}(\ell) = 1$, where the last equality holds since, by assumption, $\mathsf{val}(\Pi) > 0$. It follows Definition 3.10 that $M^{\mathsf{A}}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\ell) = 1$ and Definition 3.27 that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}(\ell) = \eta_{(\mathsf{A},j)}$. Hence, it holds that $\alpha_j = \eta_{(\mathsf{A},j)}$. Similarly, for $j \in (z-1)$, it holds that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)}(\ell) = 0$ and thus $\beta_j = 0$. Clearly, $(\mathsf{A}^{(k)}, \mathsf{B}) = \Pi$ and $\mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B}) = 1$ for every $i \in [k-1]$. We conclude that

$$\begin{aligned}
\mathrm{E}_{\langle \mathsf{A}^{(k)}, \mathsf{B}\rangle}\left[\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right] &= \mathrm{E}_{\langle \Pi\rangle}\left[\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right] \\
&= \sum_{j=0}^{z} \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}(\ell) \cdot \prod_{t=0}^{j-1}\left(1 - \widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},t)}(\ell)\right) \\
&= \sum_{j=0}^{z} \eta_{(\mathsf{A},j)} \cdot \prod_{t=0}^{j-1}\left(1 - \eta_{(\mathsf{A},t)}\right) \\
&= \sum_{j=0}^{z} \alpha_j \cdot \prod_{t=0}^{j-1}(1-\alpha_t) \\
&= \frac{\sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)}, \mathsf{B})}.
\end{aligned}$$

Induction step. Assume the lemma holds for m-round protocols and that $\mathsf{round}(\Pi) = m+1$. We prove it by the following steps: (1) we define two real vectors $\boldsymbol{\eta}_0$ and $\boldsymbol{\eta}_1$ such that the restriction of $\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$ to Π_0 and Π_1 is equal to $\widehat{L}^{\Pi_0,\boldsymbol{\eta}_0}_{\mathsf{A}}$ and $\widehat{L}^{\Pi_1,\boldsymbol{\eta}_1}_{\mathsf{A}}$, respectively; (2) we apply the induction hypothesis on the two latter measures; (3) if A controls $\mathsf{root}(\Pi)$, we use the properties of $\mathsf{A}^{(k)}$—as stated in Claim 3.4—to derive the lemma, whereas if B controls $\mathsf{root}(\Pi)$, we derive the lemma from Lemma 2.20.

All claims given in the context of this proof are proven in Section 3.7.4. We defer handling the case that $e_{\Pi}(\lambda, b) \in \{0,1\}$ for some $b \in \{0,1\}$ (see the end of this proof) and assume for now that $e_{\Pi}(\lambda, 0), e_{\Pi}(\lambda, 1) \in (0,1)$. The real vectors $\boldsymbol{\eta}_0$ and $\boldsymbol{\eta}_1$ are defined as follows.

[34] If this assumption does not hold, let $z' \in (z-1)$ be the largest index such that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z')} \neq \perp$, and let $\boldsymbol{\eta}' = \{\eta_{(\mathsf{C},j)}\}_{(\mathsf{C},j)\in[(\mathsf{A},z')]}$. It follows from Definition 3.10 that $\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)}$ is the zero measure for any $z' < j \leq z$, and thus, $\widehat{L}^{\Pi,\boldsymbol{\eta}'}_{\mathsf{A}} \equiv \widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$. Moreover, the fact that $\alpha_j = 0$ for any $z' < j \leq z$ suffices to validate the assumption.

Definition 3.29. Let $\boldsymbol{\eta}_{\mathrm{b}} = \{\eta^b_{(\mathsf{C},j)}\}_{(\mathsf{C},j)\in[(\mathsf{A},z)]}$, where for $(\mathsf{C},j) \in [(\mathsf{A},z)]$ and $b \in \{0,1\}$, let

$$\eta^b_{(\mathsf{C},j)} = \begin{cases} 0 & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) = 0; \\ \eta_{(\mathsf{C},j)} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) = 1; \\ \eta_{(\mathsf{C},j)} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b) \notin \{0,1\} \wedge (\mathsf{C} \text{ controls } \operatorname{root}(\Pi) \vee \mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b)); \\ \frac{\xi^{1-b}_{(\mathsf{C},j)}}{\xi^{b}_{(\mathsf{C},j)}} \cdot \eta_{(\mathsf{C},j)} & \text{otherwise} \end{cases},$$

where $\xi^b_{(\mathsf{C},j)} = \mathrm{E}_{\langle(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)})_b\rangle}[M^{\mathsf{C}}_{(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)})_b}]$ and $\mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b) = 1$ if $\xi^b_{(\mathsf{C},j)} \leq \xi^{1-b}_{(\mathsf{C},j)}$.[35]

Given the real vector $\boldsymbol{\eta}_{\mathrm{b}}$, consider that the dominated submeasure sequence $\boldsymbol{\eta}_{\mathrm{b}}$ induces on the subprotocol Π_b. At first glance, the relation of this submeasure sequence to the dominated submeasure sequence that $\boldsymbol{\eta}$ induces on Π is unclear; nonetheless, we manage to prove the following key observation.

Claim 3.30. *It holds that* $\widehat{L}^{\Pi_b,\boldsymbol{\eta}_{\mathrm{b}}}_{\mathsf{A}} \equiv (\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}})_b$ *for both* $b \in \{0,1\}$.

Namely, taking $(\mathsf{A},z,\boldsymbol{\eta}_{\mathrm{b}})$-$\mathsf{DMS}(\Pi_b)$—the dominated submeasures defined with respect to Π_b and $\boldsymbol{\eta}_{\mathrm{b}}$—and constructing from it the measure $\widehat{L}^{\Pi_b,\boldsymbol{\eta}_{\mathrm{b}}}_{\mathsf{A}}$ results in the same measure as taking $(\mathsf{A},z,\boldsymbol{\eta})$-$\mathsf{DMS}(\Pi)$—the dominated submeasures defined with respect to Π and $\boldsymbol{\eta}$—and constructing from it the measure $\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}$ while restricting the latter to Π_b.

Given the above fact, we can use our induction hypothesis on the subprotocols Π_0 and Π_1 with respect to the real vectors $\boldsymbol{\eta}_0$ and $\boldsymbol{\eta}_1$, respectively. For $b \in \{0,1\}$ and $j \in (z)$, let $\alpha^b_j := \mu^{\Pi_b,\boldsymbol{\eta}_{\mathrm{b}}}_{(\mathsf{A},j)}$ $(:= \mathrm{E}_{\langle(\widehat{\Pi_b})^{\boldsymbol{\eta}_{\mathrm{b}}}_{(\mathsf{A},j)}\rangle}[\widehat{M}^{\Pi_b,\boldsymbol{\eta}_{\mathrm{b}}}_{(\mathsf{A},j)}])$, and for $j \in (z-1)$, let $\beta^b_j := \mu^{\Pi_b,\boldsymbol{\eta}_{\mathrm{b}}}_{(\mathsf{B},j)}$. Assuming that $\mathsf{val}(\Pi_1) > 0$, then

$$\mathrm{E}_{\left\langle\left(\mathsf{A}^{(k)},\mathsf{B}\right)_1\right\rangle}\left[\left(\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right)_1\right] \overset{(1)}{=} \mathrm{E}_{\left\langle\mathsf{A}^{(k)}_{\Pi_1},\mathsf{B}_{\Pi_1}\right\rangle}\left[\widehat{L}^{\Pi_1,\boldsymbol{\eta}_1}_{\mathsf{A}}\right] \overset{(2)}{\geq} \frac{\sum_{j=0}^{z} \alpha^1_j \prod_{t=0}^{j-1}(1-\beta^1_t)^{k+1}(1-\alpha^1_t)}{\prod_{i=0}^{k-1} \mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}, \tag{23}$$

where (1) follows from Proposition 3.5 and Claim 3.30 and (2) follows from the induction hypothesis. Similarly, if $\mathsf{val}(\Pi_0) > 1$, then

$$\mathrm{E}_{\left\langle\left(\mathsf{A}^{(k)},\mathsf{B}\right)_0\right\rangle}\left[\left(\widehat{L}^{\Pi,\boldsymbol{\eta}}_{\mathsf{A}}\right)_0\right] = \mathrm{E}_{\left\langle\mathsf{A}^{(k)}_{\Pi_0},\mathsf{B}_{\Pi_0}\right\rangle}\left[\widehat{L}^{\Pi_0,\boldsymbol{\eta}_0}_{\mathsf{A}}\right] \geq \frac{\sum_{j=0}^{z} \alpha^0_j \prod_{t=0}^{j-1}(1-\beta^0_t)^{k+1}(1-\alpha^0_t)}{\prod_{i=0}^{k-1} \mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}. \tag{24}$$

In the following, we use the fact that the dominated submeasure sequence of one of the subprotocols is at least as long as the submeasure sequence of the protocol itself. Specifically, we show the following.

Definition 3.31. For $b \in \{0,1\}$, let $z^b = \min\{\{j \in (z) : \alpha^b_j = 1 \vee \beta^b_j = 1\} \cup \{z\}\}$.

Assuming without loss of generality (and throughout the proof of the lemma) that $z^1 \leq z^0$, we have the following claim (proven in Section 3.7.4).

Claim 3.32. *Assume that* $z^1 \leq z^0$, *and then* $z^0 = z$.

We are now ready to prove the lemma by separately considering which party controls the root of Π.

A **controls** $\operatorname{root}(\Pi)$ **and** $\mathsf{val}(\Pi_0), \mathsf{val}(\Pi_1) > 0$. Under these assumptions, we can apply the induction hypothesis on both subtrees (namely, we can use Equations (23) and (24)). Let

[35] Note that the definition of η^b follows the same lines of the definition of the dominated measure (given in Definition 3.10).

$p = e_{\Pi}(\lambda, 0)$. Compute

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] && (25)\\
&= e_{(\mathsf{A}^{(k)},\mathsf{B})}(\lambda,0)\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + e_{(\mathsf{A}^{(k)},\mathsf{B})}(\lambda,1)\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\overset{(1)}{=} p\cdot \frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right]\\
&\quad + (1-p)\cdot \frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}\cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\overset{(2)}{\geq} p\cdot \frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot \frac{\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}\\
&\quad + (1-p)\cdot \frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}\cdot \frac{\sum_{j=0}^{z}\alpha_j^1\prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}(1-\alpha_t^1)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}\\
&= \frac{p\cdot\left(\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} + \frac{(1-p)\cdot\left(\sum_{j=0}^{z}\alpha_j^1\prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}(1-\alpha_t^1)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})},
\end{aligned}$$

where (1) follows from Claim 3.4 and (2) follows from Equations (23) and (24).

Our next step is to establish a connection between the above $\{\alpha_j^0, \alpha_j^1\}_{j\in(z)}$ and $\{\beta_j^0, \beta_j^1\}_{j\in(z-1)}$ to $\{\alpha_j\}_{j\in(z)}$ and $\{\beta_j\}_{j\in(z-1)}$ (appearing in the lemma's statement). We prove the following claims.

Claim 3.33. *If* A *controls* root(Π), *it holds that* $\beta_j^0 = \beta_j$ *for every* $j \in (z-1)$ *and* $\beta_j^1 = \beta_j$ *for every* $j \in (z^1 - 1)$.

It is a direct implication of Proposition 3.13 that $\beta_j^0 = \beta_j^1 = \beta_j$ for $j \in (z^1 - 1)$. Moreover, $\beta_j^0 = \beta_j$ for every $z^1 \leq j \leq z - 1$. The latter is harder to grasp without the technical proof of the claim, which is provided in Section 3.7.4.

Claim 3.34. *If* A *controls* root(Π) *and* $z^1 < z$, *it holds that* $\alpha_{z^1}^1 = 1$.

By Claim 3.33, it follows that as long as an undefined protocol was not reached in one of the subprotocols, then $\beta_j^0 = \beta_j^1 = \beta_j$. Assuming that $z^1 < z$ and $\beta_{z^1}^1 = 1$, it would have followed that $\beta_{z^1} = 1$, and an undefined protocol is reached in the original protocol before z, a contradiction to our assumption. (Again, see Section 3.7.4 for the formal proof.)

Claims 3.33 and 3.34 and Equation (25) yield that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=0}^{z}\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}\left(p\cdot\alpha_j^0\prod_{t=0}^{j-1}(1-\alpha_t^0) + (1-p)\cdot\alpha_j^1\cdot\prod_{t=0}^{j-1}(1-\alpha_t^1)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}. \quad (26)$$

The proof of this case is concluded by plugging the next claim into Equation (26).

Claim 3.35. *If* A *controls* root(Π), *it holds that*

$$\alpha_j\cdot\prod_{t=0}^{j-1}(1-\alpha_t) = p\cdot\alpha_j^0\cdot\prod_{t=0}^{j-1}(1-\alpha_t^0) + (1-p)\cdot\alpha_j^1\cdot\prod_{t=1}^{j-1}(1-\alpha_t^1)$$

for any $j \in (z)$.

Claim 3.35 is proven in Section 3.7.4, but informally it holds since the probability of visiting the left-hand (right-hand, respectively) subprotocol in the conditional protocol $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}$ (in which α_j is defined) is $p \cdot \prod_{t=0}^{j-1}(1-\alpha_t^0)/\prod_{t=0}^{j-1}(1-\alpha_t)$ $((1-p)\cdot\prod_{t=0}^{j-1}(1-\alpha_t^1)/\prod_{t=0}^{j-1}(1-\alpha_t)$, respectively). Since α_j is defined to be the expected value of some measure in the above conditional protocol, its value is a linear combination of α_j^0 and α_j^1, with the coefficient being the above probabilities.

A **controls** $\mathsf{root}(\Pi)$ **and** $\mathsf{val}(\Pi_0) > \mathsf{val}(\Pi_1) = 0$. Under these assumptions, we can still use the induction hypothesis for the left-hand subprotocol Π_0, where for right-hand subprotocol Π_1, we argue the following.

Claim 3.36. *If* $\mathsf{val}(\Pi_1) = 0$, *it holds that* $(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}})_1 \equiv 0$.[36]

Claim 3.36 holds since according to Claim 3.30, we can simply argue that $\widehat{L}_{\mathsf{A}}^{\Pi_1,\boldsymbol{\eta}_1}$ is the zero measure, and this holds since the latter measure is a combination of A-dominated measures, all of which are the zero measure in a zero-value protocol.

Using Claim 3.36, similar computations to the ones in Equation (25) yield that

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (27)\\
&= e_{(\mathsf{A}^{(k)},\mathsf{B})}(\lambda,0)\cdot \mathrm{E}_{\langle(\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + e_{(\mathsf{A}^{(k)},\mathsf{B})}(\lambda,1)\cdot \mathrm{E}_{\langle(\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\geq p\cdot\frac{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\mathsf{A}^{(i)},\mathsf{B}\right)}\cdot\frac{\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}\\
&= \frac{p\cdot\left(\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)\right)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}.
\end{aligned}$$

Using a similar argument to that of Equation (26), combining Claim 3.33 and Equation (27) yields that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=0}^{z}\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}\left[p\cdot\alpha_j^0\prod_{t=0}^{j-1}(1-\alpha_t^0)\right]}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})}. \qquad (28)$$

The proof of this case is concluded by plugging the next claim (proven in Section 3.7.4) into Claim 3.35 and plugging the result into Equation (28).

Claim 3.37. *If* $\mathsf{val}(\Pi_1) = 0$, *it holds that* $\alpha_j^1 = 0$ *for every* $j \in (z)$.

A **controls** $\mathsf{root}(\Pi)$ **and** $\mathsf{val}(\Pi_1) > \mathsf{val}(\Pi_0) = 0$. The proof of the lemma under these assumptions is analogous to the previous case.

We have concluded the proof for cases in which A controls $\mathsf{root}(\Pi)$ and now proceed to prove the cases in which B controls $\mathsf{root}(\Pi)$. Roughly speaking, A and B switched roles, and claims true before regarding β_j are now true for α_j, and vice versa. Moreover, the analysis above relies on the probabilities that the recursive biased-continuation attacker visits the subprotocols Π_0 and Π_1 when it plays the role of A and controls $\mathsf{root}(\Pi)$. When B controls $\mathsf{root}(\Pi)$, however, these probabilities do not change (namely, they remain p and $1-p$, respectively). To overcome this difficulty, we use a convex-type argument stated in Lemma 2.20.

[36] That is, $(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}})_1$ is the zero measure.

B **controls** $\mathrm{root}(\Pi)$ **and** $\mathrm{val}(\Pi_0), \mathrm{val}(\Pi_1) > 0$. In this case, Equations (23) and (24) hold. Compute

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (29)\\
&= p \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_0\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + (1-p) \cdot \mathrm{E}_{\langle (\mathsf{A}^{(k)},\mathsf{B})_1\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right]\\
&\geq p \cdot \frac{\sum_{j=0}^{z} \alpha_j^0 \prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1} \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)} + (1-p) \cdot \frac{\sum_{j=0}^{z} \alpha_j^1 \prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}(1-\alpha_t^1)}{\prod_{i=0}^{k-1} \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)},
\end{aligned}$$

where the inequality follows from Equations (23) and (24). If B controls $\mathrm{root}(\Pi)$, we can prove the next claims (proven in Section 3.7.4), analogous to Claims 3.33 and 3.34.

Claim 3.38. *If* B *controls* $\mathrm{root}(\Pi)$*, it holds that* $\alpha_j^0 = \alpha_j$ *for every* $j \in (z)$ *and that* $\alpha_j^1 = \alpha_j$ *for every* $j \in (z^1)$*.*

Claim 3.39. *If* B *controls* $\mathrm{root}(\Pi)$ *and* $z^1 < z$*, it holds that* $\beta_{z^1}^1 = 1$*.*

Claim 3.38 and Equation (29) yield that

$$\begin{aligned}
&\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \qquad (30)\\
&\geq \sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t)\left(p \cdot \frac{\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1} \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)} + (1-p) \cdot \frac{\prod_{t=0}^{j-1}(1-\beta_t^1)^{k+1}}{\prod_{i=0}^{k-1} \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)}\right).
\end{aligned}$$

Applying the convex-type inequality given in Lemma 2.20 for each summand in the right-hand side of Equation (30) with respect to $x = \prod_{t=0}^{j-1}(1-\beta_t^0)$, $y = \prod_{t=0}^{j-1}(1-\beta_t^1)$, $a_i = \mathrm{val}(\mathsf{A}^{(i-1)},\mathsf{B}_0)$, $b_i = \mathrm{val}(\mathsf{A}^{(i-1)},\mathsf{B}_1)$, $p_0 = p$, and $p_1 = 1-p$ and plugging into Equation (30) yield that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\alpha_t)\left(p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0) + (1-p) \cdot \prod_{t=0}^{j-1}(1-\beta_t^1)\right)^{k+1}}{\prod_{i=0}^{k-1}\left(p \cdot \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right) + (1-p) \cdot \mathrm{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_1\right)\right)}. \qquad (31)$$

We conclude the proof of this case by observing that for every $i \in (k-1)$, it holds that $\mathrm{val}(\mathsf{A}^{(i)},\mathsf{B}) = p \cdot \mathrm{val}((\mathsf{A}^{(i)},\mathsf{B})_0) + (1-p) \cdot \mathrm{val}((\mathsf{A}^{(i)},\mathsf{B})_1)$ and using the next claim (proven in Section 3.7.4), analogous to Claim 3.35.

Claim 3.40. *If* B *controls* $\mathrm{root}(\Pi)$*, it holds that*

$$\prod_{t=0}^{j-1}(1-\beta_t) = p \cdot \prod_{t=0}^{j-1}(1-\beta_t^0) + (1-p) \cdot \prod_{t=0}^{j-1}(1-\beta_t^1).$$

B **controls** $\mathrm{root}(\Pi)$ **and** $\mathrm{val}(\Pi_0) > \mathrm{val}(\Pi_1) = 0$. In this case, Claims 3.33 and 3.38 yield that $\alpha_j = 0$ for any $j \in (z^1)$. Hence, it suffices to prove that

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \frac{\sum_{j=z^1+1}^{z} \alpha_j \prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1} \mathrm{val}(\mathsf{A}^{(i)},\mathsf{B})}. \qquad (32)$$

Thus, the proof immediately follows if $z^1 = z$, and in the following we assume that $z^1 < z$.

As in Equation (29), compute

$$\begin{aligned} \mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] &= p\cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_0\right\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_0\right] + (1-p)\cdot \mathrm{E}_{\left\langle \left(\mathsf{A}^{(k)},\mathsf{B}\right)_1\right\rangle}\left[\left(\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right)_1\right] \\ &\geq p\cdot \frac{\sum_{j=0}^{z}\alpha_j^0\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}(1-\alpha_t^0)}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}, \end{aligned} \tag{33}$$

where the inequality follows Equation (24) and Claim 3.36. Claim 3.38 now yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=0}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\alpha_t)\cdot \frac{p\cdot\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}, \tag{34}$$

where Claim 3.38 yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=z^1+1}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\alpha_t)\cdot \frac{p\cdot\prod_{t=0}^{j-1}(1-\beta_t^0)^{k+1}}{\prod_{i=0}^{k-1}\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}. \tag{35}$$

Multiplying both the numerator and the denominator for every summand of Equation (35) with p^k yields

$$\mathrm{E}_{\langle \mathsf{A}^{(k)},\mathsf{B}\rangle}\left[\widehat{L}_{\mathsf{A}}^{\Pi,\boldsymbol{\eta}}\right] \geq \sum_{j=z^1+1}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\alpha_t)\cdot \frac{\left(p\cdot\prod_{t=0}^{j-1}(1-\beta_t^0)\right)^{k+1}}{\prod_{i=0}^{k-1}p\cdot\mathsf{val}\left(\left(\mathsf{A}^{(i)},\mathsf{B}\right)_0\right)}. \tag{36}$$

Equation (32), and hence the proof of this case, is derived by observing that $\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B}) = p\cdot\mathsf{val}((\mathsf{A}^{(i)},\mathsf{B})_0)$ for every $i\in(k-1)$[37] and plugging Claims 3.39 and 3.40 into Equation (36).

B **controls** $\mathsf{root}(\Pi)$ **and** $\mathsf{val}(\Pi_1) > \mathsf{val}(\Pi_0) = 0$. Analogously to Claim 3.37, it holds that $\alpha_j^0 = 0$ for every $j\in(z)$. Claim 3.38 yields that $\alpha_j = 0$ for every $j\in(z)$. The proof of this case trivially follows since

$$\frac{\sum_{j=0}^{z}\alpha_j\prod_{t=0}^{j-1}(1-\beta_t)^{k+1}(1-\alpha_t)}{\prod_{i=0}^{k-1}\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})} = 0.$$

The above case analysis concludes the proof of the lemma when assuming that $e_\Pi(\lambda,b)\notin\{0,1\}$ for both $b\in\{0,1\}$. Assume that $e_\Pi(\lambda,b)=1$ for some $b\in\{0,1\}$. Since, by assumption, $\mathsf{val}(\Pi)>0$, it follows that $\mathsf{val}(\Pi_b)>0$. Moreover, the definition of conditional protocols (Definition 3.17) yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b)=1$ and $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,1-b)=0$ for any $(\mathsf{C},j)\in[(\mathsf{A},z)]$ (regardless of which party controls $\mathsf{root}(\Pi)$). By defining $\boldsymbol{\eta}_{\mathbf{b}}=\boldsymbol{\eta}$, the definition of the dominated measure (Definition 3.10) yields that $\alpha_j=\alpha_j^b$ for every $j\in(z)$ and that $\beta_j=\beta_j^b$ for every $j\in(z-1)$. The proof of this case immediately follows from the induction hypothesis on Π_b. □

3.7.4 Missing Proofs. This section is dedicated to proving deferred statements used in the proof of Lemma 3.28. We assume a fixed protocol Π, a fixed real vector $\boldsymbol{\eta} = (\eta_{(\mathsf{A},0)},\eta_{(\mathsf{B},0)},\ldots,\eta_{(\mathsf{B},z-1)},\eta_{(\mathsf{A},z)})$, and a fixed positive integer k. We also assume that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},z)}\neq\perp$, $z^1\leq z^0$ and $e_\Pi(\lambda,b)\in(0,1)$ for both $b\in\{0,1\}$. Recall that we defined two real vectors $\boldsymbol{\eta}_{\mathbf{0}}$ and $\boldsymbol{\eta}_{\mathbf{1}}$ (Definition 3.29), and for $b\in\{0,1\}$ we defined $\alpha_j^b := \mu_{(\mathsf{A},j)}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}}$ $(:= \mathrm{E}_{\langle(\widehat{\Pi_b})^{\boldsymbol{\eta}_{\mathbf{b}}}_{(\mathsf{A},j)}\rangle}[\widehat{M}_{(\mathsf{A},j)}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}}])$ for $j\in(z)$, and $\beta_j^b := \mu_{(\mathsf{B},j)}^{\Pi_b,\boldsymbol{\eta}_{\mathbf{b}}}$ for $j\in(z-1)$.

[37] Recall that if $\mathsf{val}(\mathsf{A},\mathsf{B})=0$, then $\mathsf{val}(\mathsf{A}^{(i)},\mathsf{B})=0$ for every $i\in\mathbb{N}$.

We begin with the following proposition, which underlies many of the claims to follow.

Proposition 3.41. *For $b \in \{0,1\}$ and $(\mathsf{C}, j) \in [(\mathsf{A}, z)]$, it holds that*

(1) $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b = (\widehat{\Pi_b})^{\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{C},j)}$*; and*
(2) $\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b \equiv \widehat{M}^{\Pi_b,\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{C},j)}$.

Namely, the restriction of $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ (the (C, j)'th conditional protocol with respect to Π and $\boldsymbol{\eta}$) to its bth subtree is equal to the (C, j)'th conditional protocol defined with respect to Π_b (bth subtree of Π) and $\boldsymbol{\eta}_\mathbf{b}$. Moreover, the result of multiplying the C-dominated measure of $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}$ by $\eta_{(\mathsf{C},j)}$, and then restricting it to the subtree $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b$, is equivalent to multiplying the C-dominated measure of $(\widehat{\Pi_b})^{\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{C},j)}$ by $\eta^b_{(\mathsf{C},j)}$.[38]

Proof of Proposition 3.41. The proof is by induction on the ordered pairs $[(\mathsf{A}, z)]$.

Base case. Recall that the first pair of $[(\mathsf{A}, z)]$ is $(\mathsf{A}, 0)$. Definition 3.27 yields that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},0)} = \Pi$ and that $(\widehat{\Pi_b})^{\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{A},0)} = \Pi_b$, yielding that Item 1 holds for $(\mathsf{A}, 0)$. As for Item 2, by Definition 3.10 and the assumption that $e_\Pi(\lambda, b) \in (0, 1)$ for both $b \in \{0, 1\}$, it holds that

$$\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},0)}\right)_b \equiv \left(\eta_{(\mathsf{A},0)} \cdot M^{\mathsf{A}}_{\Pi}\right)_b \equiv \begin{cases} \eta_{(\mathsf{A},0)} \cdot M^{\mathsf{A}}_{\Pi_b} & \mathsf{A} \text{ controls } \mathsf{root}(\Pi) \lor \mathsf{Smaller}_{\Pi}(b); \\ \eta_{(\mathsf{A},0)} \cdot \frac{\xi^{1-b}_{(\mathsf{A},0)}}{\xi^{b}_{(\mathsf{A},0)}} \cdot M^{\mathsf{A}}_{\Pi_b} & \text{otherwise.} \end{cases}$$

The proof that Item 2 holds for $(\mathsf{A}, 0)$ now follows from Definition 3.29.

Induction step. Fix $(\mathsf{C}, j) \in [(\mathsf{A}, z)]$ and assume the claim holds for $\mathsf{pred}(\mathsf{C}, j)$. Using the induction hypothesis, we first prove Item 1 for (C, j). Next, using the fact that Item 1 holds for (C, j), we prove Item 2.

Proving Item 1. By Definition 3.27, it holds that

$$\begin{aligned} \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b &= \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)} |\neg\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)\right)_b \\ &= \left(\widehat{\Pi}^{\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)_b |\neg\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{\mathsf{pred}(\mathsf{C},j)}\right)_b \\ &\overset{(1)}{=} \left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta}_\mathrm{b}}_{\mathsf{pred}(\mathsf{C},j)} |\neg\left(\widehat{M}^{\Pi_b,\boldsymbol{\eta}_\mathrm{b}}_{\mathsf{pred}(\mathsf{C},j)}\right) \\ &= \left(\widehat{\Pi_b}\right)^{\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{C},j)}, \end{aligned}$$

where (1) follows from the induction hypothesis.

[38] Note that Item 1 is not immediate. Protocol $\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b$ is a restriction of a protocol defined on the root of Π, whereas $(\widehat{\Pi_b})^{\boldsymbol{\eta}_\mathrm{b}}_{(\mathsf{C},j)}$ is a protocol defined on the root of Π_b.

Proving Item 2. Similarly to the base case, Definition 3.10 yields that

$$\left(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b \equiv \begin{cases} 0 & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b)=0;\\ \eta_{(\mathsf{C},j)}\cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b)=1;\\ \eta_{(\mathsf{C},j)}\cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(\lambda,b)\notin\{0,1\}\wedge\\ & \left(\mathsf{C}\text{ controls }\mathsf{root}(\Pi)\vee\mathsf{Smaller}_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}}(b)\right);\\ \eta_{(\mathsf{C},j)}\cdot\frac{\xi^{1-b}_{(\mathsf{C},j)}}{\xi^{b}_{(\mathsf{C},j)}}\cdot M^{\mathsf{C}}_{\left(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{C},j)}\right)_b} & \text{otherwise,}\end{cases}$$

and the proof follows from Item 1 and Definition 3.29. □

Recall that the real numbers α^b_j and β^b_j were defined to be the expected values of the (A,j)'th and (B,j)'th dominated measures in the sequence $(\mathsf{A},z,\boldsymbol{\eta}_\mathbf{b})$-$\mathsf{DMS}(\Pi_b)$, respectively (see the proof of Lemma 3.28). Following Proposition 3.41, we could equivalently define α^b_j and β^b_j with respect to the sequence $(\mathsf{A},z,\boldsymbol{\eta})$-$\mathsf{DMS}(\Pi)$.

Proposition 3.42. *For both $b\in\{0,1\}$, it holds that*

(1) $\alpha^b_j = \mathrm{E}_{\langle(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)})_b\rangle}[(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{A},j)})_b]$ *for every $j\in(z)$; and*

(2) $\beta^b_j = \mathrm{E}_{\langle(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)})_b\rangle}[(\widehat{M}^{\Pi,\boldsymbol{\eta}}_{(\mathsf{B},j)})_b]$ *for every $j\in(z-1)$.*

Proof. Immediately follows Proposition 3.41. □

Proposition 3.42 allows us to use Proposition 3.13 in order to analyze the connections between α^0_j and α^1_j to α_j, and similarly between β^0_j and β^1_j to β_j. Toward this goal, we analyze the edge distribution of the conditional protocols defined in the procedure that generates the measure sequence $(\mathsf{A},z,\boldsymbol{\eta})$-$\mathsf{DMS}(\Pi)$.

Proposition 3.43. *The following holds for both $b\in\{0,1\}$:*

(1) A *controls* $\mathsf{root}(\Pi)\Rightarrow$

  (a) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda,b)=e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}(1-\alpha^b_t)}{\prod_{t=0}^{j-1}(1-\alpha_t)}$ *for all $j\in(z)$.*

  (b) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda,b)=e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j}(1-\alpha^b_t)}{\prod_{t=0}^{j}(1-\alpha_t)}$ *for all $j\in(z-1)$.*

(2) B *controls* $\mathsf{root}(\Pi)\Rightarrow$

  (a) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda,b)=e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}(1-\beta^b_t)}{\prod_{t=0}^{j-1}(1-\beta_t)}$ *for all $j\in(z)$.*

  (b) $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j)}}(\lambda,b)=e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}(1-\beta^b_t)}{\prod_{t=0}^{j-1}(1-\beta_t)}$ *for all $j\in(z-1)$.*

Proof. We prove Item 1 using induction on the ordered pairs $[(\mathsf{A},z)]$. The proof of Item 2 is analogous.

Base case. The proof follows since according to Definition 3.27, it holds that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},0)}=\Pi$.

Induction step. Fix $(\mathsf{C},j)\in[(\mathsf{A},z)]$ and assume the claim holds for $\mathsf{pred}(\mathsf{C},j)$. The proof splits according to which party C is.

Case $\mathsf{C}=\mathsf{A}$. If $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B},j-1)}}(\lambda,b)=0$, Definition 3.17 yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A},j)}}(\lambda,b)=0$. The proof follows since, by the induction hypothesis, it holds that

$$e_{\widehat{\Pi}^{\eta}_{(\mathrm{A},j)}}(\lambda,b) = e_{\widehat{\Pi}^{\eta}_{(\mathrm{B},j-1)}}(\lambda,b) = e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j-1}(1-\alpha_t)}.$$

In the complementary case, i.e., $e_{\widehat{\Pi}^{\eta}_{(\mathrm{B},j-1)}}(\lambda,b) > 0$, Proposition 3.13 and Definition 3.10 yield that $\beta_{j-1} = \beta_{j-1}^b$. It must be the case that $\beta_{j-1} = \beta_{j-1}^b < 1$, since otherwise, according to Definition 3.27, it holds that $\widehat{\Pi}^{\eta}_{(\mathrm{A},j)} =\perp$, a contradiction to the assumption that $\widehat{\Pi}^{\eta}_{(\mathrm{A},z)} \neq\perp$. The proof follows since in this case Definition 3.17 and Proposition 3.42 yield that

$$\begin{aligned} e_{\widehat{\Pi}^{\eta}_{(\mathrm{A},j)}}(\lambda,b) &= e_{\widehat{\Pi}^{\eta}_{(\mathrm{B},j-1)}}(\lambda,b)\cdot\frac{1-\beta_{j-1}^b}{1-\beta_{j-1}} \\ &= e_{\widehat{\Pi}^{\eta}_{(\mathrm{B},j-1)}}(\lambda,b) \\ &= e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j-1}(1-\alpha_t)}, \end{aligned}$$

where the last equality follows the induction hypothesis.

Case $\mathrm{C} = \mathrm{B}$. It must be the case that $\alpha_j < 1$, since otherwise, similarly to the previous case and according to Definition 3.27, it holds that $\widehat{\Pi}^{\eta}_{(\mathrm{B},j)} =\perp$, a contradiction to the assumption that $\widehat{\Pi}^{\eta}_{(\mathrm{A},z)} \neq\perp$. The proof follows since in this case Definition 3.17 and Proposition 3.42 yield that

$$\begin{aligned} e_{\widehat{\Pi}^{\eta}_{(\mathrm{B},j)}}(\lambda,b) &= e_{\widehat{\Pi}^{\eta}_{(\mathrm{A},j)}}(\lambda,b)\cdot\frac{1-\alpha_j^b}{1-\alpha_j} \\ &= e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j-1}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j-1}(1-\alpha_t)}\cdot\frac{1-\alpha_j^b}{1-\alpha_j} \\ &= e_{\Pi}(\lambda,b)\cdot\frac{\prod_{t=0}^{j}\left(1-\alpha_t^b\right)}{\prod_{t=0}^{j}(1-\alpha_t)}, \end{aligned}$$

where the second equality follows from the induction hypothesis. □

Using the above propositions, we now turn our focus to proving the claims in the proof of Lemma 3.28. To facilitate reading and tracking the proof, we cluster claims together according to their role in the proof of Lemma 3.28.

Proving Claims 3.30 and 3.32.

Proof of Claim 3.30. For $b \in \{0,1\}$, it holds that

$$\begin{aligned} \widehat{L}_{\mathrm{A}}^{\Pi_b,\eta_b} &\equiv \sum_{j=0}^{z} \widehat{M}_{(\mathrm{A},j)}^{\Pi_b,\eta_b}\cdot\prod_{t=0}^{j-1}\left(1-\widehat{M}_{(\mathrm{A},t)}^{\Pi_b,\eta_b}\right) \\ &\equiv \sum_{j=0}^{z}\left(\widehat{M}_{(\mathrm{A},j)}^{\Pi,\eta}\right)_b\cdot\prod_{t=0}^{j-1}\left(1-\left(\widehat{M}_{(\mathrm{A},t)}^{\Pi,\eta}\right)_b\right) \\ &\equiv \left(\widehat{L}_{\mathrm{A}}^{\Pi,\eta}\right)_b, \end{aligned}$$

where the second equivalence follows from Proposition 3.41. □

Proof of Claim 3.32. Assume toward a contradiction that $z^0 < z$. By the definition of z^0 (Definition 3.31) and the definition of conditional protocols (Definition 3.17), it follows that $(\widehat{\Pi_0})^{\eta_0}_{(\mathsf{A}, z^0+1)} =\perp$. Since (by assumption) $z^1 \leq z^0$, it also holds that $(\widehat{\Pi_1})^{\eta_1}_{(\mathsf{A}, z^0+1)} =\perp$. Hence, Proposition 3.41 yields that $(\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z^0+1)})_0, (\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z^0+1)})_1 =\perp$. Namely, the function describing $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z^0+1)}$ does not correspond to any two-party execution when restricting it to the subtrees $\mathcal{T}(\Pi_0)$ and $\mathcal{T}(\Pi_1)$. Hence, the aforementioned function does not correspond to a two-party execution (over $\mathcal{T}(\Pi)$), in contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z)} \neq\perp$. □

Proving Claims 3.33 to 3.35. The following proofs rely on the next observation. As long as $\alpha^b_j < 1$ and $\beta^b_j < 1$, Proposition 3.43 ensures that there is a positive probability to visit both the left and the right subtree of the (C, j)'th conditional protocol.

Proof of Claim 3.34. Assume that A controls $\mathsf{root}(\Pi)$ and that $z^1 < z$. Assume toward a contradiction that $\alpha^1_{z^1} < 1$. Since $z^1 \leq z^0$ (by assumption), it follows that $\alpha^0_{z^1} < 1$ as well. The definition of z^1 (Definition 3.31) yields that $\beta^1_{z^1} = 1$. However, Proposition 3.43 yields that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B}, j)}}(\lambda, b) \in (0, 1)$ for both $b \in \{0, 1\}$, and thus Propositions 3.13 and 3.42 yield that $\beta_{z^1} = 1$. Now, Definition 3.27 yields that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z^1+1)} =\perp$, a contradiction to the assumption that $\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{A}, z)} \neq\perp$. □

Proof of Claim 3.33. For $j \in (z^1 - 1)$, it holds that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B}, j)}}(\lambda, b) \in (0, 1)$ for both $b \in \{0, 1\}$. Thus, $\beta^0_j = \beta^1_j = \beta_j$ is a direct implication of Propositions 3.13 and 3.41.

For $z^1 \leq z - 1$, Claim 3.34 and Proposition 3.43 yield that $e_{\widehat{\Pi}^{\boldsymbol{\eta}}_{(\mathsf{B}, j)}}(\lambda, 0) = 1$. Since, by Definition 3.29, it holds that $\eta_{(\mathsf{B}, j)} = \eta^0_{(\mathsf{B}, j)}$, Definition 3.10 and Proposition 3.41 yield that $\beta^0_j = \beta_j$. □

Proof of Claim 3.35. The proof immediately follows from Propositions 3.42 and 3.43. □

Proving Claims 3.36 and 3.37.

Proof of Claim 3.36. By Definition 3.10, it holds that $\widehat{M}^{\Pi_1, \boldsymbol{\eta}_1}_{(\mathsf{A}, j)} \equiv 0$ for every $j \in (z)$. Definition 3.27 yields that $\widehat{L}^{\Pi_1, \boldsymbol{\eta}_1}_{\mathsf{A}} \equiv 0$. The proof follows from Claim 3.30. □

Proof of Claim 3.37. Follows similar arguments to the above proof of Claim 3.36, together with Proposition 3.42. □

Proving Claims 3.38 to 3.40. The proofs of the rest of the claims stated in the proof of Lemma 3.28 are analogous to the claims proven above. Specifically, Claim 3.38 is analogous to Claim 3.33, Claim 3.39 is analogous to Claim 3.34, and Claim 3.40 is analogous to Claim 3.35.

3.8 Proving Lemma 3.26

Lemma 3.26 immediately follows by the next lemma.

Lemma 3.44. *For every protocol* Π, *there exists* $(\mathsf{C}, j) \in \{\mathsf{A}, \mathsf{B}\} \times \mathbb{N}$ *such that*

$$\mathrm{E}_{\langle \Pi_{(\mathsf{C}, j)} \rangle}\left[M^{\mathsf{C}}_{\Pi_{(\mathsf{C}, j)}}\right] = 1.$$

The proof of Lemma 3.44 is given below, but first we use it to derive Lemma 3.26.

Proof of Lemma 3.26. Let z be the minimal integer such that $\sum_{j=0}^{z} \alpha_j \geq c$ or $\sum_{j=0}^{z} \beta_j \geq c$. Note that such z is guaranteed to exist by Lemma 3.44, and since by Lemma 3.12 it holds that $\alpha_j = \mathrm{E}_{\langle \Pi_{(\mathsf{A}, j)} \rangle}[M^{\mathsf{A}}_{\Pi_{(\mathsf{A}, j)}}]$ and $\beta_j = \mathrm{E}_{\langle \Pi_{(\mathsf{B}, j)} \rangle}[M^{\mathsf{B}}_{\Pi_{(\mathsf{B}, j)}}]$, the proof splits to the following cases.

Case $\sum_{j=0}^{z} \alpha_j \geq c$. By the choice of z, it holds that $\sum_{j=0}^{z-1} \alpha_j < c$ and $\sum_{j=0}^{z-1} \beta_j < c$. Lemma 3.24 yields that

$$\begin{aligned} \mathrm{E}_{\langle \Pi \rangle}\left[L_{\Pi}^{\mathsf{A},z}\right] &= \sum_{j=0}^{z} \alpha_j \prod_{t=0}^{j-1} (1-\beta_t)(1-\alpha_t) \\ &\overset{(1)}{\geq} \sum_{j=0}^{z} \alpha_j \prod_{t=0}^{z-1} (1-\beta_t)(1-\alpha_t) \\ &\overset{(2)}{\geq} \left(\sum_{j=0}^{z} \alpha_j\right) \cdot \left(1 - \sum_{j=0}^{z-1} \beta_j\right) \cdot \left(1 - \sum_{j=0}^{z-1} \alpha_j\right) \\ &\overset{(3)}{\geq} c \cdot (1-2c), \end{aligned}$$

where (1) follows from multiplying the jth summand by $\prod_{t=j}^{z-1}(1-\beta_t)(1-\alpha_t) \leq 1$ and (2) and (3) follow since $(1-x)(1-y) \geq 1-(x+y)$ for any $x, y \geq 0$. Hence, z satisfies Item 1.

Case $\sum_{j=0}^{z} \alpha_j < c$. By the choice of z, it holds that $\sum_{j=0}^{z} \beta_j \geq c$ and $\sum_{j=0}^{z-1} \beta_j < c$. Similar arguments to the previous case show that z satisfies Item 2. □

Toward proving Lemma 3.44, we prove that there is always a leaf for which the value of the dominated measure is 1.

Claim 3.45. *Let* Π *be a protocol with* $\mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. *Then there exists* $\ell \in \mathcal{L}_1(\Pi)$ *such that* $M_{\Pi}^{\mathsf{A}}(\ell) = 1$.

Proof. The proof is by induction on the round complexity of Π.

Assume that $\mathsf{round}(\Pi) = 0$ and let ℓ be the only node in $\mathcal{T}(\Pi)$. Since $\mathsf{OPT}_{\mathsf{A}}(\Pi) > 0$, it must be the case that $\chi_{\Pi}(\ell) = 1$. The proof follows since Definition 3.10 yields that $M_{\Pi}^{\mathsf{A}}(\ell) = 1$.

Assume that $\mathsf{round}(\Pi) = m+1$ and that the lemma holds for m-round protocols. If $e_{\Pi}(\lambda, b) = 1$ for some $b \in \{0,1\}$, then by Proposition 3.8, it holds that $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. This allows us to apply the induction hypothesis on Π_b, which yields that there exists $\ell \in \mathcal{L}_1(\Pi_b)$ such that $M_{\Pi_b}^{\mathsf{A}}(\ell) = 1$. In this case, according to Definition 3.10, $M_{\Pi}^{\mathsf{A}}(\ell) = M_{\Pi_b}^{\mathsf{A}}(\ell) = 1$, and the proof follows.

In the following, we assume that $e_{\Pi}(\lambda, b) \in (0,1)$ for any $b \in \{0,1\}$. We conclude the proof using the following case analysis.

A **controls** $\mathsf{root}(\Pi)$. According to Proposition 3.8, there exists $b \in \{0,1\}$ such that $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$. This allows us to apply the induction hypothesis on Π_b, which yields that there exists $\ell \in \mathcal{L}_1(\Pi_b)$ such that $M_{\Pi_b}^{\mathsf{A}}(\ell) = 1$. The A-maximal property of M_{Π}^{A} (Proposition 3.13(1)) yields that $M_{\Pi}^{\mathsf{A}}(\ell) = M_{\Pi_b}^{\mathsf{A}}(\ell) = 1$, and the proof for this case follows.

B **controls** $\mathsf{root}(\Pi)$. According to Proposition 3.8, $\mathsf{OPT}_{\mathsf{A}}(\Pi_b) = \mathsf{OPT}_{\mathsf{A}}(\Pi) = 1$ for both $b \in \{0,1\}$. This allows us to apply the induction hypothesis on Π_0 and Π_1, which yields that there exists $\ell_0 \in \mathcal{L}_1(\Pi_0)$ and $\ell_1 \in \mathcal{L}_1(\Pi_1)$ such that $M_{\Pi_0}^{\mathsf{A}}(\ell_0) = 1$ and $M_{\Pi_1}^{\mathsf{A}}(\ell_1) = 1$. The B-minimal property of M_{Π}^{A} (Proposition 3.13(2)) yields that there exists $b \in \{0,1\}$ such that $M_{\Pi}^{\mathsf{A}}(\ell_b) = M_{\Pi_b}^{\mathsf{A}}(\ell_b) = 1$ (the bit b for which $\mathsf{Smaller}_{\Pi}(b) = 1$), and the proof for this case follows.

This concludes the case analysis and the proof follows. □

We can now derive Lemma 3.44. Claim 3.45 and Proposition 3.13 yield that the number of possible transcripts of $\Pi_{(\mathsf{C},j)}$ shrinks as (C, j) grows. Specifically, at least one possible transcript of $\Pi_{(\mathsf{A},j)}$ whose common outcome is 1 (the transcript represented by the leaf is guaranteed to exist from Claim 3.45) is *not* a possible transcript of $\Pi_{(\mathsf{B},j)}$. Similarly, at least one possible transcript of $\Pi_{(\mathsf{B},j-1)}$ whose common outcome is 0 is not a possible transcript of $\Pi_{(\mathsf{A},j)}$. Since the number of possible transcripts of Π is finite (though might be exponentially large), there exists $j \in \mathbb{N}$ such that either the common outcome of all possible transcripts $\Pi_{(\mathsf{A},j)}$ is 1 or the common outcome of all possible transcripts of $\Pi_{(\mathsf{B},j)}$ is 0. The expected value of the A-dominated measure of $\Pi_{(\mathsf{A},j)}$ or the B-dominated measure of $\Pi_{(\mathsf{B},j)}$ will be 1. The formal proof is given next.

Proof of Lemma 3.44. Assume toward a contradiction that $\mathrm{E}_{\langle \Pi_{(\mathsf{C},j)}\rangle}[M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}] < 1$ for every $(\mathsf{C},j) \in \{\mathsf{A},\mathsf{B}\} \times \mathbb{N}$. It follows that $\Pi_{(\mathsf{C},j)} \neq \perp$ for every such (C,j). For a pair $(\mathsf{C},j) \in \{\mathsf{A},\mathsf{B}\} \times \mathbb{N}$, recursively define $\mathcal{L}_{(\mathsf{C},j)} := \mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cup \mathcal{S}_{(\mathsf{C},j)}$, where $\mathcal{S}_{(\mathsf{C},j)} := \{\ell \in \mathcal{L}(\Pi) : M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}(\ell) = 1\}$ and $\mathcal{L}_{(\mathsf{B},-1)} := \emptyset$. The following claim (proven below) shows two properties of $\mathcal{S}_{(\mathsf{C},j)}$.

Claim 3.46. *It holds that* $\mathcal{S}_{(\mathsf{C},j)} \neq \emptyset$ *and* $\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cap \mathcal{S}_{(\mathsf{C},j)} = \emptyset$ *for every* $(\mathsf{C},j) \succeq (\mathsf{B},0)$.

Claim 3.46 yields that $|\mathcal{L}_{(\mathsf{C},j)}| > |\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)}|$ for every $(\mathsf{C},j) \succeq (\mathsf{B},0)$, a contradiction to the fact that $\mathcal{L}_{(\mathsf{C},j)} \subseteq \mathcal{L}(\Pi)$ for every (C,j). □

Proof of Claim 3.46. Let $(\mathsf{C},j) \succeq (\mathsf{B},0)$. By Lemma 3.21, it holds that $\mathrm{OPT}_{\mathsf{C}}(\Pi_{(\mathsf{C},j)}) = 1$.[39] Hence, Claim 3.45 yields that $\mathcal{S}_{(\mathsf{C},j)} \neq \emptyset$.

Toward proving the second property, let $\ell' \in \mathcal{L}_{\mathsf{pred}(\mathsf{C},j)}$, and let $(\mathsf{C}',j') \in [\mathsf{pred}(\mathsf{C},j)]$ such that $\ell' \in \mathcal{S}_{(\mathsf{C}',j')}$. By the definition of $\mathcal{S}_{(\mathsf{C}',j')}$, it holds that $M^{\mathsf{C}'}_{\Pi_{(\mathsf{C}',j')}}(\ell') = 1$. By Proposition 3.19, it holds that $\ell' \notin \mathrm{Supp}(\langle \Pi_{(\mathsf{C}'',j'')}\rangle)$ for every $(\mathsf{C}'',j'') \succ (\mathsf{C}',j')$. Since $(\mathsf{C},j) \succ \mathsf{pred}(\mathsf{C},j) \succeq (\mathsf{C}',j')$, it holds that $\ell' \notin \mathrm{Supp}(\langle \Pi_{(\mathsf{C},j)}\rangle)$. By Definition 3.10, it holds that $M^{\mathsf{C}}_{\Pi_{(\mathsf{C},j)}}(\ell) = 0$ for every $\ell \notin \mathrm{Supp}(\langle \Pi_{(\mathsf{C},j)}\rangle)$, and thus $\ell' \notin \mathcal{S}_{(\mathsf{C},j)}$. Hence, $\mathcal{L}_{\mathsf{pred}(\mathsf{C},j)} \cap \mathcal{S}_{(\mathsf{C},j)} = \emptyset$. □

4 EFFICIENTLY BIASING COIN-FLIPPING PROTOCOLS

In Section 3, we showed that for any coin-flipping protocol and $\varepsilon \in (0, \frac{1}{2}]$, applying the biased-continuation attack recursively for $\kappa = \kappa(\varepsilon)$ times biases the honest party's outcome by (at least) $1/2 - \varepsilon$. Implementing this attack, however, requires access to a sampling algorithm (i.e., the biased continuator BiasedCont; see Definition 3.1), which we do not know how to efficiently implement even when assuming OWFs do not exist. In this section, we show that the inexistence of OWFs does suffice to implement an *approximation* of the biased-continuation attack that can be used to implement a strong enough variant of the aforementioned attack.

The outline of this section is as follows. In Section 4.1, we define the *approximated (recursive) biased-continuation attacker*, an approximated variant of the (ideal) recursive biased-continuation attacker defined in Section 3. We show that this approximated attacker does well as long as it does not visits *low-value nodes*—the expected protocol's outcome conditioned on visiting the nodes (transcripts) is close to zero. In Section 4.2, we define a special class of protocols, called *approximately pruned protocols*, that have (almost) no low-value nodes. We conclude that the approximated attacker does well when it attacks approximately pruned protocols, and argue about the implementation of this attacker. In Section 4.3, we define the *pruning-in-the-head attacker* that behaves as if the protocol it is attacking is pruned, and by doing so manages to make use of the recursive approximated biased-continuation attacker to attack *any* protocol. In Section 4.4, we argue about the implementation of the pruning-in-the-head attacker. Finally, in Section 4.5, we show that the assumption that OWFs do not exist implies that the above attacker can be implemented efficiently,

[39] Note that this might not hold for $\Pi_{(\mathsf{A},0)} = \Pi$. Namely, it might be the case that $\mathrm{OPT}_{\mathsf{B}}(\Pi) = 1$. In this case, M^{A}_{Π} is the zero measure, $\Pi_{(\mathsf{B},0)} = \Pi$, and $\mathcal{S}_{(\mathsf{A},0)} = \emptyset$.

yielding that the outcome on *any* coin-flipping protocol can be efficiently biased to be arbitrarily close to 0 or 1.

Throughout the section, as was the case in Section 3, we prove statements with respect to attackers that, when playing the role of the left-hand party of the protocol (i.e., A), are trying to bias the common output of the protocol toward one, and, when playing the role of the right-hand party of the protocol (i.e., B), are trying to bias the common output of the protocol toward zero. All statements have analog ones with respect to the opposite attack goals.

4.1 The Approximated Biased-Continuation Attacker

We start with defining the recursive approximated biased-continuation attacker, an approximated variant of the recursive biased-continuation attacker defined in Section 3, and state our bound on its success probability. The rest of the section will be devoted to proving this bound.

Defining the attacker. The approximated recursive biased-continuation attacker is using an approximated version of the biased continuator BiasedCont (see Definition 3.1). The approximated biased continuator is only guaranteed to work well when applied on nodes whose value (i.e., the probability that the protocol outcome is 1 given that the current transcript is the node's label) is not too close to the borders. The motivation for using this weaker biased continuator is that, as we see later, it can be efficiently implemented assuming the inexistence of OWFs. In the following, let $\mathsf{BiasedCont}_\Pi$ be as in Definition 3.1.

Definition 4.1 (Low-value and High-value Nodes). For a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ and $\delta \in [0, 1]$, let

- $\mathcal{S}\mathsf{mall}_\Pi^\delta = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{val}(\Pi_u) \leq \delta\}$, and
- $\mathcal{L}\mathsf{arge}_\Pi^\delta = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{val}(\Pi_u) \geq 1 - \delta\}$.

For $\mathsf{C} \in \{\mathsf{A}, \mathsf{B}\}$, let $\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{C}} = \mathcal{S}\mathsf{mall}_\Pi^\delta \cap \mathcal{C}\mathsf{trl}_\Pi^\mathsf{C}$ and similarly let $\mathcal{L}\mathsf{arge}_\Pi^{\delta,\mathsf{C}} = \mathcal{L}\mathsf{arge}_\Pi^\delta \cap \mathcal{C}\mathsf{trl}_\Pi^\mathsf{C}$.[40]

Definition 4.2 (Approximated Biased Continuator $\mathsf{BiasedCont}_\Pi^{\xi,\delta}$*).* Algorithm C is a (ξ, δ)-biased-continuator for an m-round protocol Π if the following hold:

$$(1)\ \Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \begin{array}{c} \mathrm{SD}(\mathsf{C}(\ell_{1,\ldots,i}, 1), \mathsf{BiasedCont}_\Pi(\ell_{1,\ldots,i}, 1)) > \xi \\ \wedge\ \ell_{1,\ldots,i} \notin \mathcal{S}\mathsf{mall}_\Pi^\delta \end{array}\right] \leq \xi,$$

and

$$(2)\ \Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \begin{array}{c} \mathrm{SD}(\mathsf{C}(\ell_{1,\ldots,i}, 0), \mathsf{BiasedCont}_\Pi(\ell_{1,\ldots,i}, 0)) > \xi \\ \wedge\ \ell_{1,\ldots,i} \notin \mathcal{L}\mathsf{arge}_\Pi^\delta \end{array}\right] \leq \xi.$$

Let $\mathsf{BiasedCont}_\Pi^{\xi,\delta}$ be an arbitrary (but fixed) (ξ, δ)-biased continuator of Π.

The recursive approximated biased-continuation attacker is identical to that defined in Section 3, except that it uses the approximated biased-continuator sampler and not the ideal one.

Let $\mathsf{A}_\Pi^{(0,\xi,\delta)} \equiv \mathsf{A}$, and for integer $i > 0$, define:

ALGORITHM 4.3 (APPROXIMATED RECURSIVE BIASED-CONTINUATION ATTACKER $\mathsf{A}_\Pi^{(i,\xi,\delta)}$).

```
Parameters: integer $i > 0$, $\xi, \delta \in (0, 1)$.
Input: transcript $u \in \{0, 1\}^*$.
Operation:
    (1) If $u \in \mathcal{L}(\Pi)$, output $\chi_\Pi(u)$ and halt.
    (2) Set $\mathsf{msg} = \mathsf{BiasedCont}^{\xi,\delta}_{(\mathsf{A}_\Pi^{(i-1,\xi,\delta)},\mathsf{B})}(u, 1)$.
```

[40] Recall that $\mathcal{C}\mathsf{trl}_\Pi^\mathsf{C}$ denotes the nodes in $\mathcal{T}(\Pi)$ controlled by party C (see Definition 2.4).

(3) *Send* msg *to* B.
(4) *If* $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$, *output* $\chi_\Pi(u')$.

In the following, we sometimes refer to the base (nonrecursive) version of the above algorithm, i.e., $\mathsf{A}_\Pi^{(1,\xi,\delta)}$, as the approximated biased-continuation attacker. When clear from the context, we will remove the protocol name (i.e., Π) from the subscript of the above attacker. (As a rule of thumb, in statements and definitions, we explicitly write the protocols to which the algorithms refer, whereas in proofs and informal discussions we usually omit them.)

The attacker's success probability.. We would like to bound the difference between the biased-continuation attacker and its approximated variant defined above. Following Definition 4.2, if the approximated biased continuator $\mathsf{BiasedCont}^{\xi,\delta}$ is called on non-low-value nodes (transcripts), both attackers are given similar answers, so the difference between them will be small. Hence, as long as the probability of hitting low-value nodes under A's control is small (note that only nodes under A's control are queried), we expect that the recursive approximated biased-continuation attacker will do well. This is formally put in the next lemma.

Lemma 4.4. *For any* $\delta \in (0, 1/4]$ *and* $k \in \mathbb{N}$, *there exists a polynomial* $p_{k,\delta}$ *such that the following holds. Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be an m-round protocol, and assume that* $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{1.5\delta',\mathsf{A}})] \le \alpha$ *for some* $\delta \le \delta' \le \frac{1}{4}$.[41] *Then for any* $\xi, \mu \in (0, 1)$, *it holds that*

$$SD\left(\left\langle \mathsf{A}_\Pi^{(k)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_\Pi^{(k,\xi,\delta')}, \mathsf{B}\right\rangle\right) \le \phi_{k,\delta}^{\mathsf{It}}(\alpha, \xi, m, \delta', \mu) := (\alpha + \xi) \cdot p_{k,\delta}(m, 1/\delta', 1/\mu) + \mu.$$

The fact that the lemma assumes a bound with respect to $\mathcal{S}\mathsf{mall}_\Pi^{1.5\delta',\mathsf{A}}$ (and not $\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}}$) is of a technical nature and is not significant to the understating of the statement.

We will use Lemma 4.4 as follows: the constants δ, δ', and k will be set according to the (constant) bias of the protocol. Then we choose $\mu \in o(1)$. Finally, we are free to choose α and ξ to be $1/p$ for large enough polynomial p, such that $p \gg p_{k,\delta}(m, 1/\delta', 1/\mu)$.

In addition to Lemma 4.4, the following lemma will be useful when considering pruned protocols in the next section.

Lemma 4.5. *For any* $\delta \in (0, 1/4]$ *and* $k \in \mathbb{N}$, *there exists a polynomial* $q_{k,\delta}$ *such that the following holds. Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *and* $\Pi' = (\mathsf{C}, \mathsf{D})$ *be two m-round protocols and let* $\mathcal{F}$ *be a frontier of* $\mathcal{U}$, *for some* $\mathcal{U} \subseteq \mathcal{V}(\Pi)$. *Assume* $SD(\langle\Pi\rangle, \langle\Pi'\rangle) \le \varepsilon$, $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{1.5\delta',\mathsf{A}})] \le \alpha$ *for some* $\delta \le \delta' \le \frac{1}{4}$, *and* $\Pr_{\langle\Pi'\rangle}[\mathsf{desc}(\mathcal{F})] \le \beta$. *Then, for any* $\xi, \mu \in (0, 1)$, *it holds that*

$$\Pr_{\left\langle \mathsf{A}_\Pi^{(k,\delta',\xi)}, \mathsf{B}\right\rangle}[\mathsf{desc}(\mathcal{F})] \le \phi_{k,\delta}^{\mathsf{Bal}}(\alpha, \beta, \varepsilon, m, \delta', \mu) + \phi_{k,\delta}^{\mathsf{It}}(\alpha, \xi, m, \delta', \mu),$$

for

$$\phi_{k,\delta}^{\mathsf{Bal}}(\alpha, \beta, \varepsilon, m, \delta', \mu) := (\alpha + \beta + \varepsilon) \cdot q_{k,\delta}(m, 1/\delta', 1/\mu) + \mu.$$

Namely, Lemma 4.5 asserts that if the transcripts of Π and Π′ are close, the probability of hitting low-value nodes in Π under the control of the left-hand party is small and the probability of hitting a frontier $\mathcal{F}$ in Π′ is small as well. Then the probability of hitting this frontier in Π when the recursive approximated biased-continuation attacker is taking the role of the left-hand party in Π is small as well.

Outline for the proof of Lemma 4.4. Proving Lemma 4.4 actually turns out to be quite challenging. The lemma assumes that the probability, according to the *honest distribution* of leaves (i.e., ⟨Π⟩),

[41] $\mathsf{desc}(\mathcal{S})$ is the set of nodes with ancestor in $\mathcal{S}$ (see Definition 2.1).

to generate a low-value node under A's control is small. The queries the attacker makes, however, might be chosen from a different distribution, making some nodes much more likely to be queried than before. We call such nodes "unbalanced." If low-value nodes under A's control were a large fraction of the unbalanced ones, then Definition 4.2 guarantees nothing about the answers of the approximated biased continuator $\mathsf{BiasedCont}^{\xi,\delta}$. Indeed, the main technical contribution of this section is to show that low-value nodes under A's control are only a small fraction of the unbalanced ones.

A natural approach for proving Lemma 4.4 is to use induction on k. The base case when $k = 1$ holds since $\mathsf{BiasedCont}_{\Pi}^{\xi,\delta'}$, used by $\mathsf{A}_{\Pi}^{(1,\xi,\delta')}$, is a (ξ,δ')-biased continuator of Π. Moving to the induction step, we assume the lemma is true for $k-1$. Namely, we assume that

$$\mathrm{SD}\left(\left\langle \mathsf{A}_{\Pi}^{(k-1)},\mathsf{B}\right\rangle,\left\langle \mathsf{A}_{\Pi}^{(k-1,\xi,\delta')},\mathsf{B}\right\rangle\right) \text{ is small.} \tag{37}$$

The first step is to apply the ideal biased-continuation attacker on the left-hand side part of both protocols. We will show that even after applying the attacker, the protocols remain close. Namely, we will prove the following statement:

$$\begin{aligned} &\mathrm{SD}\left(\left\langle \mathsf{A}_{\Pi}^{(k-1)},\mathsf{B}\right\rangle,\left\langle \mathsf{A}_{\Pi}^{(k-1,\xi,\delta')},\mathsf{B}\right\rangle\right) \text{ is small} \\ &\Rightarrow \mathrm{SD}\left(\left\langle \left(\mathsf{A}_{\Pi}^{(k-1)}\right)^{(1)},\mathsf{B}\right\rangle,\left\langle \left(\mathsf{A}_{\Pi}^{(k-1,\xi,\delta')}\right)^{(1)},\mathsf{B}\right\rangle\right) \text{ is small as well.} \end{aligned} \tag{38}$$

Putting it differently, to prove Equation (38), we show that the biased-continuation attacker is "robust"—it does not make similar protocols dissimilar.

The second step it to show that applying the ideal biased-continuation attacker on the right-hand-side protocol is similar to applying the approximated biased-continuation attacker on the same protocol. Namely, we will prove the following statement:

$$\mathrm{SD}\left(\left\langle \left(\mathsf{A}_{\Pi}^{(k-1,\xi,\delta')}\right)^{(1)},\mathsf{B}\right\rangle,\left\langle \left(\mathsf{A}_{\Pi}^{(k-1,\xi,\delta')}\right)^{(1,\xi,\delta')},\mathsf{B}\right\rangle\right) \text{ is small.} \tag{39}$$

Putting it differently, to prove the "ideal to real" reduction described in Equation (38), we show that the approximated biased-continuation attacker is a good approximation to its ideal variant.

In fact, both the "robustness" property (Equation (38)) and the "ideal to real" reduction (Equation (39)) require the additional assumption that the probability of hitting low-value nodes under the control of the left-hand-side party is small. Following the induction hypothesis (Equation (37)), showing this assumption to be true reduces to showing that the recursive ideal biased-continuation attacker hits low-value nodes under its control with only small probability (specifically, we need this to hold for $k-1$ recursions). The lemma assumes that the probability of hitting such nodes in the original protocol is small, namely, that the set of A-controlled low-value nodes is of low density. We will show that the recursive ideal biased-continuation attacker does not increase the density of any sets by much.

The outline of this section is as follows. In Section 4.1.1, we formally define unbalanced nodes with respect to the *nonrecursive* attacker and show that low-value nodes under A's control are only a small fraction of them. This connection between unbalanced nodes to low-value ones underlines all the other results in this section. In Section 4.1.2, we state and prove the "robustness" property. In Section 4.1.3, we analyze the "ideal to real" reduction. In Section 4.1.4, we show that when it is applied recursively, the ideal biased-continuation attacker does not increase the probability of hitting low-density sets. Finally, in Section 4.1.5, we give the proofs of Lemmas 4.4 and 4.5.

4.1.1 Unbalanced Nodes. For non-low-value and non-high-value transcripts, Definition 4.2 guarantees that when queried on transcripts chosen according to the honest distribution of leaves (i.e., $\langle \Pi \rangle$), there is only a small statistical distance between the answers of the biased continuator BiasedCont and its approximated variant $\mathsf{BiasedCont}^{\xi,\delta}$. The queries the biased-continuation attacker makes, however, might be chosen from a different distribution, making some transcripts much more likely to be queried than before. We call such transcripts "unbalanced."

Definition 4.6 (Unbalanced Nodes). For a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ and $\gamma \geq 1$, let $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{v}_{(\mathsf{A}_{\Pi}^{(1)}, \mathsf{B})}(u) \geq \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)\}$, where $\mathsf{A}_{\Pi}^{(1)}$ is as in Algorithm 3.2 and v as in Definition 2.4.[42]

Namely, $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$ are those nodes that a random execution of $(\mathsf{A}^{(1)}, \mathsf{B})$ visits with probability at least γ times the probability that a random execution of Π does.

Given a protocol $\Pi = (\mathsf{A}, \mathsf{B})$, we would like to understand what makes a node unbalanced. Let u be a γ-unbalanced node, i.e., $\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u) \geq \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)$. By the edge distribution of $(\mathsf{A}^{(1)}, \mathsf{B})$ ((Claim 3.4), it follows that

$$\frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)} = \prod_{\substack{0 \leq i \leq |u|-1 : \\ u_{1,\ldots,i} \in \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{A}}}} \frac{\mathsf{val}(\Pi_{u_{1,\ldots,i+1}})}{\mathsf{val}(\Pi_{u_{1,\ldots,i}})} \geq \gamma. \tag{40}$$

Hence, if γ is large, one of the terms of the product in Equation (40) must be large. Since the value of any subprotocol is at most one, the numerator of each term cannot be large. It then must be the case that the denominator of at least one of those terms is close to zero, i.e., that u has a low-value ancestor controlled by A.[43]

The following key lemma formulates the above intuition and shows that the biased-continuation attacker does not bias the original distribution of the protocol by too much, unless it has previously visited a low-value node controlled by A.

Lemma 4.7. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol and let* $\mathsf{A}_{\Pi}^{(1)}$ *be as in Algorithm 3.2. Then, for every* $\delta \in (0, \frac{1}{2}]$, *there exists a constant* $c = c(\delta) > 0$, *such that for every* $\delta' \geq \delta$ *and* $\gamma > 1$*:*

$$\Pr_{\langle \mathsf{A}_{\Pi}^{(1)}, \mathsf{B} \rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right)\right] \leq \frac{2}{\gamma^{c}}.^{44}$$

Namely, the probability of reaching a γ-unbalanced node that does not have a δ'-low ancestor, for $\delta' \geq \delta$, is some inverse polynomial in γ. The proof of Lemma 4.7 is given below. Looking ahead, we will apply this lemma for some $\gamma \in \mathrm{poly}(n)$, where n is the security parameter given to the parties. At a high level, $\mathsf{BiasedCont}^{\xi,\delta}$ gives a good (enough) approximation for the biased continuator BiasedCont when called on nodes that are at most $\mathrm{poly}(n)$-unbalanced. This lemma is useful since it gives a $1/\mathrm{poly}(n)$ bound for the probability that $\mathsf{BiasedCont}^{\xi,\delta}$ is called on nodes that are more than $\mathrm{poly}(n)$-unbalanced. Another important point is that the inverse polynomial (i.e., c) depends only on δ (and is independent of γ and δ'). This becomes crucial when analyzing the success probability of the approximated biased-continuation attacker.

Lemma 4.7 allows us to bound the probability that the (ideal) biased-continuation attacker hits unbalanced nodes with the probability that the *original* protocol hits A-controlled low-value nodes.

[42] $\mathsf{v}_{\mathsf{T}}(u)$ is the probability that node (transcript) u is reached in an (honest) execution of protocol T.

[43] This discussion is not entirely accurate, but it gives a good intuition for why unbalanced nodes relate to low-value ones. Indeed, the actual statement (Lemma 4.7) shows this discussion to hold only with high probability, which suffices for our needs.

[44] Recall that for $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, $\overline{\mathsf{desc}}(\mathcal{S})$ stands for the set of nodes that have an ancestor in $\mathcal{S}$ but are not in $\mathcal{S}$ itself (see Definition 2.1).

Indeed, consider the first time $(\mathsf{A}^{(1)}, \mathsf{B})$ reaches a γ-unbalanced node u. If an A-controlled low-value ancestor node was reached before reaching u, then this ancestor cannot be γ-unbalanced, and thus the probability of hitting it (and in turn hitting u) is bounded by γ times the probability of the original protocol hitting A-controlled low-value nodes. In the complementary case, in which no A-controlled low-value node was reached before reaching u, the probability of hitting u is bounded by Lemma 4.7. This analysis is where we use that Lemma 4.7 is proven with respect to *proper* descendants of low-value nodes. The above discussion is stated formally next.

Lemma 4.8. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a protocol, let* $\delta \in (0, \frac{1}{2}]$*, and let* $c = c(\delta)$ *be according to Lemma 4.7. Then*

$$\Pr_{\langle \mathsf{A}_\Pi^{(1)}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma\right)\right] \leq \gamma \cdot \Pr_{\langle \mathsf{A}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}}\right)\right] + \frac{2}{\gamma^c},$$

for any $\delta' \geq \delta$ *and* $\gamma > 1$.

Proof. By Proposition 2.2, it holds that

$$\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma\right) \subseteq \operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}} \setminus \mathcal{U}\mathsf{nBal}_\Pi^\gamma\right) \cup \operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}}\right)\right). \tag{41}$$

We can now compute

$$\begin{aligned}\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma\right)\right] &\leq \Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}} \setminus \mathcal{U}\mathsf{nBal}_\Pi^\gamma\right)\right] \\ &\quad + \Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}}\right)\right)\right] \\ &\leq \gamma \cdot \Pr_{\langle \mathsf{A}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}}\right)\right] + \frac{2}{\gamma^c},\end{aligned}$$

where the second inequality follows from the definition of $\mathcal{U}\mathsf{nBal}_\Pi^\gamma$ and Lemma 4.7. □

The rest of this section is dedicated to proving Lemma 4.7.

Proving Lemma 4.7.

Proof of Lemma 4.7. The lemma is proven via proving the following facts:

(1) There exists $c > 0$ such that

$$\Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B}\rangle}\left[\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}\right)\right)\right] \leq \frac{2 - \mathsf{val}(\Pi)}{\gamma^c} \tag{42}$$

for every $\gamma > 1$. Note that Equation (42) only considers descendants of $\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}$, and not proper descendants.

(2) For $\gamma > 1$, it holds that

$$\operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}\right)\right) \subseteq \operatorname{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \operatorname{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}\right)\right).[45] \tag{43}$$

(3) For $\delta' > \delta$, it holds that

$$\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta', \mathsf{A}}\right) \subseteq \mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}\right). \tag{44}$$

It is clear that combining the above steps yields (a stronger version of) the lemma.

Proof of (1): Fix $\delta \in (0, \frac{1}{2}]$ and let $c := \alpha(\delta)$ be the value guaranteed in Lemma 2.21. The proof is by induction on the round complexity of Π.

[45] It thus follows that $\operatorname{desc}(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \overline{\operatorname{desc}}(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}})) = \operatorname{desc}(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \operatorname{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta, \mathsf{A}}))$.

Assume $\mathsf{round}(\Pi) = 0$ and let ℓ be the single leaf of Π. By Definition 4.6, $\ell \notin \mathcal{U}\mathsf{nBal}_\Pi^\gamma$ and thus $\mathcal{U}\mathsf{nBal}_\Pi^\gamma = \emptyset$. Hence, for every $\delta > 0$,

$$\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}})\right)\right] = \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}[\emptyset] = 0 \le \frac{2-\mathsf{val}(\Pi)}{\gamma^c}.$$

Assume that Equation (42) holds for m-round protocols and that $\mathsf{round}(\Pi) = m+1$. If $e_{(\mathsf{A},\mathsf{B})}(\lambda, b) = 1$ for some $b \in \{0,1\}$ (recall that λ denotes the empty string); then

$$\begin{aligned}&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}})\right)\right]\\ &\quad= \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_b\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_b}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_b}^{\delta,\mathsf{A}})\right)\right]\\ &\quad= \Pr_{\left\langle \mathsf{A}^{(1)}_{\Pi_b},\mathsf{B}_{\Pi_b}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_b}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_b}^{\delta,\mathsf{A}})\right)\right],\end{aligned}$$

where the second equality follows Proposition 3.5. The proof now follows from the induction hypothesis.

To complete the proof, we assume that $e_{(\mathsf{A},\mathsf{B})}(\lambda, b) \notin \{0,1\}$ for both $b \in \{0,1\}$, and let $p = e_{(\mathsf{A},\mathsf{B})}(\lambda, 0)$. The proof splits according to who controls the root of Π.

B **controls** $\mathsf{root}(\Pi)$. We first note that

$$\begin{aligned}&\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}}\right)\\ &\quad= \left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^\gamma \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right)\right) \cup \left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^\gamma \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}}\right)\right).\end{aligned} \tag{45}$$

To see the above, first note $\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}}) \setminus \{\mathsf{root}(\Pi)\} = \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}) \cup \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}})$, and since B controls $\mathsf{root}(\Pi)$, it holds that $\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \{\mathsf{root}(\Pi)\} = \mathcal{U}\mathsf{nBal}_{\Pi_0}^\gamma \cup \mathcal{U}\mathsf{nBal}_{\Pi_1}^\gamma$. Finally, since $\gamma > 1$, it holds that $\mathsf{root}(\Pi) \notin \mathcal{U}\mathsf{nBal}_\Pi^\gamma$, and Equation (45) follows.

We can now write

$$\begin{aligned}&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}}\right)\right)\right]\\ &\quad= e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0)\cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}})\right)\right]\\ &\qquad+ e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1)\cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_1\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}})\right)\right]\\ &\quad= p\cdot \Pr_{\left\langle \mathsf{A}^{(1)}_{\Pi_0},\mathsf{B}_{\Pi_0}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}})\right)\right]\\ &\qquad+ (1-p)\cdot \Pr_{\left\langle \mathsf{A}^{(1)}_{\Pi_1},\mathsf{B}_{\Pi_1}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}})\right)\right]\\ &\quad\le p\cdot\frac{2-\mathsf{val}(\Pi_0)}{\gamma^c} + (1-p)\cdot\frac{2-\mathsf{val}(\Pi_1)}{\gamma^c}\\ &\quad= \frac{2-\mathsf{val}(\Pi)}{\gamma^c}.\end{aligned}$$

The first equality follows from Equation (45), the second equality follows from Proposition 3.5, and the inequality follows from the induction hypothesis.

A **controls** $\mathsf{root}(\Pi)$. If $\mathsf{val}(\Pi) \le \delta$, then $\mathsf{root}(\Pi) \in \mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}}$. Therefore, $\mathcal{U}\mathsf{nBal}_\Pi^\gamma \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}}) = \emptyset$ and the proof follows from a similar argument as in the base case.

In the complementary case, i.e., $\mathsf{val}(\Pi) > \delta$, assume without loss of generality that $\mathsf{val}(\Pi_0) \geq \mathsf{val}(\Pi) \geq \mathsf{val}(\Pi_1)$. We start with the case that $\mathsf{val}(\Pi_1) > 0$. For $b \in \{0,1\}$, let $\gamma_b := \frac{\mathsf{val}(\Pi)}{\mathsf{val}(\Pi_b)} \cdot \gamma$. By Claim 3.4, for $u \in \mathcal{V}(\Pi)$ with $u \neq \mathsf{root}(\Pi)$ and $b = u_1$, it holds that

$$\frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})}(u)} = \frac{e_{(\mathsf{A},\mathsf{B})}(\lambda,b)}{e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,b)} \cdot \frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})_b}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})_b}(u)} = \frac{\mathsf{val}(\Pi_b)}{\mathsf{val}(\Pi)} \cdot \frac{\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})_b}(u)}{\mathsf{v}_{(\mathsf{A},\mathsf{B})_b}(u)}.$$

Thus, $u \in \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$ if and only if $u \in \mathcal{U}\mathsf{nBal}_{\Pi_b}^{\gamma_b}$. Hence, using also the fact that $\mathsf{root}(\Pi) \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}$ (since we assumed $\mathsf{val}(\Pi) > \delta$), arguments similar to those used to prove Equation (45) yield that

$$\begin{aligned} &\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right) \\ &\quad = \left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^{\gamma_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right)\right) \cup \left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^{\gamma_1} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}}\right)\right). \end{aligned} \tag{46}$$

Moreover, for $b \in \{0,1\}$, it holds that

$$\begin{aligned} &\Pr_{\langle(\mathsf{A}^{(1)},\mathsf{B})_b\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_b}^{\gamma_b} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_b}^{\delta,\mathsf{A}})\right)\right] \\ &\quad = \Pr_{\left\langle\mathsf{A}_{\Pi_b}^{(1)},\mathsf{B}_{\Pi_b}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_b}^{\gamma} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi_b}^{\delta,\mathsf{A}})\right)\right] \\ &\quad \leq \frac{2-\mathsf{val}(\Pi_b)}{\gamma_b^c} \\ &\quad = \left(\frac{\mathsf{val}(\Pi_b)}{\mathsf{val}(\Pi)}\right)^c \cdot \frac{2-\mathsf{val}(\Pi_b)}{\gamma^c}. \end{aligned} \tag{47}$$

The first equality follows from Proposition 3.5. The inequality follows from the next case analysis: if $\gamma_b > 1$, then it follows from the induction hypothesis applied with respect to Π_b, δ, and γ_b; if $\gamma_b \leq 1$, then it follows since $\frac{2-\mathsf{val}(\Pi_b)}{\gamma_b^c} \geq 1$ and since the left-hand side of the inequality is a probability mass. Hence,

$$\begin{aligned} &\Pr_{\langle\mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right)\right)\right] \\ &\quad = e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0) \cdot \Pr_{\langle(\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^{\gamma_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right)\right)\right] \\ &\qquad + e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1) \cdot \Pr_{\langle(\mathsf{A}^{(1)},\mathsf{B})_1\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_1}^{\gamma_1} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_1}^{\delta,\mathsf{A}}\right)\right)\right] \\ &\quad \leq p \cdot \left(\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}\right)^{1+c} \cdot \frac{2-\mathsf{val}(\Pi_0)}{\gamma^c} + (1-p) \cdot \left(\frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)}\right)^{1+c} \cdot \frac{2-\mathsf{val}(\Pi_1)}{\gamma^c}, \end{aligned} \tag{48}$$

where the equality follows from Equation (46), and the inequality follows from Equation (47) together with Claim 3.4. Letting $y = \frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} - 1$, $x = \mathsf{val}(\Pi)$, and $\lambda = \frac{p}{1-p}$, and noting that $\lambda y = (\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} - 1) \cdot \frac{p}{1-p} = \frac{p \cdot \mathsf{val}(\Pi_0) - p \cdot \mathsf{val}(\Pi)}{\mathsf{val}(\Pi) - p \cdot \mathsf{val}(\Pi)} \leq \frac{p \cdot \mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)} \leq 1$, Lemma 2.21 yields (after multiplying by $\frac{1-p}{\gamma^c}$) that

$$p \cdot \left(\frac{\mathsf{val}(\Pi_0)}{\mathsf{val}(\Pi)}\right)^{1+c} \cdot \frac{2-\mathsf{val}(\Pi_0)}{\gamma^c} + (1-p) \cdot \left(\frac{\mathsf{val}(\Pi_1)}{\mathsf{val}(\Pi)}\right)^{1+c} \cdot \frac{2-\mathsf{val}(\Pi_1)}{\gamma^c} \leq \frac{2-\mathsf{val}(\Pi)}{\gamma^c}, \tag{49}$$

completing the proof for the case $\mathsf{val}(\Pi_1) > 0$.

It is left to argue the case that $\mathsf{val}(\Pi_1) = 0$. In this case, according to Claim 3.4, it holds that $e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,0) = 1$ and $e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda,1) = 0$. Hence, there are no unbalanced nodes in Π_1, i.e., $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}) \cap \mathcal{V}(\Pi_1) = \emptyset$. As before, let $\gamma_0 := \frac{\mathsf{val}(\Pi)}{\mathsf{val}(\Pi_0)} \cdot \gamma = p \cdot \gamma$ (the latter equality holds since $\mathsf{val}(\Pi) = p \cdot \mathsf{val}(\Pi_0)$.) Arguments similar to those used to prove Equation (46) yield that

$$\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right) = \mathcal{U}\mathsf{nBal}_{\Pi_0}^{\gamma_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right). \tag{50}$$

It follows that

$$\begin{aligned}&\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right)\right)\right] \\ &\quad = e_{(\mathsf{A}^{(1)},\mathsf{B})}(\lambda, 0) \cdot \Pr_{\langle (\mathsf{A}^{(1)},\mathsf{B})_0\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_{\Pi_0}^{\gamma_0} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_0}^{\delta,\mathsf{A}}\right)\right)\right] \\ &\quad \le \left(\frac{1}{p}\right)^{1+c} \cdot \frac{2 - \mathsf{val}(\Pi_0)}{\gamma^c}.\end{aligned}$$

Applying Lemma 2.21 with the same parameters as above completes the proof.

Proof of (2): Fix $\gamma > 1$ and recall that for a set $\mathcal{S} \subset \mathcal{V}(\Pi)$, $\mathsf{frnt}(\mathcal{S})$ stands for the frontier of $\mathcal{S}$; i.e., the set of nodes belong to $\mathcal{S}$, whose ancestors do not belong to $\mathcal{S}$ (see Definition 2.1). We prove that

$$\mathsf{frnt}\left(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right)\right) \subseteq \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}\right), \tag{51}$$

and the proof of (2) follows.

Let $u \in \mathsf{frnt}(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}))$. We prove Equation (51) by showing that $u \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}$. Since $\gamma > 1$ and $u \in \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$, it is clear that $u \neq \mathsf{root}(\Pi)$. Let w be the parent of u. By the choice of u, it follows that $w \notin \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$, and thus $\mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(w) < \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(w)$. We write

$$\begin{aligned}\gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(w) \cdot e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u) &> \mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(w) \cdot e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u) \\ &= \mathsf{v}_{(\mathsf{A}^{(1)},\mathsf{B})}(u) \\ &\ge \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(u) \\ &= \gamma \cdot \mathsf{v}_{(\mathsf{A},\mathsf{B})}(w) \cdot e_{(\mathsf{A},\mathsf{B})}(w,u).\end{aligned} \tag{52}$$

We conclude that $e_{(\mathsf{A},\mathsf{B})}(w,u) < e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u)$, and thus it must be the case that w is controlled by A. By Claim 3.4, it holds that $e_{(\mathsf{A}^{(1)},\mathsf{B})}(w,u) = e_{(\mathsf{A},\mathsf{B})}(w,u) \cdot \frac{\mathsf{val}(\Pi_u)}{\mathsf{val}(\Pi_w)}$, and thus $\mathsf{val}(\Pi_u) > \mathsf{val}(\Pi_w)$. Finally, observe that $w \notin \mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}}$, since otherwise $u \in \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}})$. It follows that $\mathsf{val}(\Pi_w) > \delta$, and hence $\mathsf{val}(\Pi_u) > \delta$, as required. □

Proof of (3): Note that for every $\delta' \ge \delta$, it holds that $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}} \subseteq \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}$. Hence, $\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}) \subseteq \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta,\mathsf{A}})$, and the proof follows. □

4.1.2 *The Biased-Continuation Attacker Is Robust.*

Consider what happens when the biased-continuation attacker attacks a protocol $\Pi = (\mathsf{A},\mathsf{B})$. This attacker chooses a random 1-leaf according to $\langle \Pi \rangle$, the leaf distribution of Π. If there was another protocol Π' that was close (in the leaf distribution sense) to Π, then the attacker can instead sample from $\langle \Pi' \rangle$ while making similar decisions throughout its operation. So the biased-continuation attacker is robust to the distribution from which it samples. This is formally put in the next lemma.

Lemma 4.9 (Robustness Lemma). *Let $\Pi = (\mathsf{A},\mathsf{B})$ and $\Pi' = (\mathsf{C},\mathsf{D})$ be two m-round protocols, let $\delta \in (0, \frac{1}{2}]$, and let $c = c(\delta)$ be according to Lemma 4.7. Assuming $SD(\langle \Pi \rangle, \langle \Pi' \rangle) \le \alpha$, $\chi_\Pi \equiv \chi_{\Pi'}$, and Π and Π' have the same control scheme, it holds that*

$$SD\left(\left\langle \mathsf{A}_{\Pi}^{(1)}, \mathsf{B}\right\rangle, \left\langle \mathsf{C}_{\Pi'}^{(1)}, \mathsf{D}\right\rangle\right) \le \frac{3 \cdot m \cdot \gamma}{\delta'} \cdot \left(\alpha + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]\right) + \frac{2}{\gamma^c},$$

for every $\delta' \ge \delta$ and $\gamma \ge 1$, where $\mathsf{A}^{(1)}$ and $\mathsf{C}^{(1)}$ are as in Algorithm 3.2.

Namely, the biased-continuation attacker does not make similar protocols too dissimilar. The rest of this section is dedicated to proving Lemma 4.9.

Proof. We use Lemma 2.17. Define the random function f given an element from $\mathcal{V}(\Pi) \cup \{\perp\}$ as follows: given $u \in \mathcal{V}(\Pi)$, if A controls u, return $\ell \leftarrow \langle \Pi_u \rangle$ such that $\chi_\Pi(\ell) = 1$ (if no such node exists, return an arbitrary node in $\mathrm{desc}(u)$); otherwise, i.e., if B controls u, return $\ell \leftarrow \langle \Pi_u \rangle$. Finally, given $\perp$, f returns $\perp$. The random function g given an element from $\mathcal{V}(\Pi) \cup \{\perp\}$ is analogously defined with respect to protocol Π'.[46] For function ϕ with range in $\mathcal{L}(\Pi)$, let H^ϕ be the following algorithm:

Algorithm 4.10 (H).

```
State: node $u$, set to $\lambda$ at the start of the execution.
Operation:
    (1) Repeat for $m$ times:
        (a) Set $\ell = \phi(u)$.
        (b) Set $u = u \circ \ell_i$, where $i$ is the current iteration.
    (2) Output $u$.
```

It is easy to verify that $\mathsf{H}^f \equiv \langle \mathsf{A}_\Pi^{(1)}, \mathsf{B} \rangle$ and $\mathsf{H}^g \equiv \langle \mathsf{C}_{\Pi'}^{(1)}, \mathsf{D} \rangle$. Hence, it suffices to upper-bound $\mathrm{SD}(\mathsf{H}^f, \mathsf{H}^g)$.

For $i \in [m]$, let P_i be the ith node in a random execution of Π (such a node consists of $i-1$ bits). We use the next claim, proven below.

Claim 4.11. $\mathrm{E}_{u \leftarrow P_i}[SD(f(u), g(u))] \le \frac{2\alpha}{\delta'} + \Pr_{\langle \Pi \rangle}\left[\mathrm{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right]$.

Let Q_i denote the ith query to f in a random execution of H^f (note that by construction, such a query always exists) and let $Q = (Q_1, \ldots, Q_m)$. By construction, for $u \in \mathcal{V}(\Pi)$ with $|u| = i - 1$, $Q_i(u)$ is the probability that u is visited in a random execution of $(\mathsf{A}_\Pi^{(1)}, \mathsf{B})$. We get

$$
\begin{aligned}
\Pr_{(q_1,\ldots,q_m)\leftarrow Q}[\exists i \in [m] : q_i \neq \perp \wedge Q_i(q_i) > \gamma \cdot P_i(q_i)] &= \Pr_{\langle \mathsf{A}^{(1)}, \mathsf{B} \rangle}\left[\mathrm{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^\gamma\right)\right] \\
&\le \gamma \cdot \Pr_{\langle \Pi \rangle}\left[\mathrm{desc}\left(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}}\right)\right] + \frac{2}{\gamma^c},
\end{aligned}
$$

where the inequality follows from Lemma 4.8.

The proof of Lemma 4.9 now follows by Lemma 2.17, letting $k = m$, $a = \frac{2\alpha}{\delta'} + \Pr_{\langle \Pi \rangle}[\mathrm{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}})]$, $\lambda = \gamma$, and $b = \gamma \cdot \Pr_{\langle \Pi \rangle}[\mathrm{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta',\mathsf{A}})] + \frac{2}{\gamma^c}$. □

Proof of Claim 4.11. Let $\mathcal{V}_i(\Pi) = \{v \in \mathcal{V}(\Pi) : |v| = i - 1\}$, $\mathcal{V}_i^{\mathsf{A}}(\Pi) = \mathcal{V}_i(\Pi) \cap \mathcal{C}\mathsf{trl}_\Pi^{\mathsf{A}}$, and $\mathcal{V}_i^{\mathsf{B}}(\Pi) = \mathcal{V}_i(\Pi) \cap \mathcal{C}\mathsf{trl}_\Pi^{\mathsf{B}}$. Compute

$$
\begin{aligned}
\mathrm{E}_{u \leftarrow P_i}[\mathrm{SD}(f(u), g(u))] &= \sum_{u \in \mathcal{V}_i(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)) \qquad (53) \\
&= \sum_{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)) + \sum_{u \in \mathcal{V}_i^{\mathsf{B}}(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)).
\end{aligned}
$$

[46] The sets $\mathcal{V}(\Pi)$ and $\mathcal{V}(\Pi')$, as well as the sets $\mathcal{L}(\Pi)$ and $\mathcal{L}(\Pi')$, are identical, as both describe nodes in the complete binary tree of height m. See Section 2 for further details.

In the rest of the proof, we show that

$$\sum_{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)) \leq \frac{1}{\delta'} \cdot \sum_{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi)} P_i(u) \cdot \mathrm{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle) + \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}\right)\right], \tag{54}$$

that

$$\sum_{u \in \mathcal{V}_i^{\mathsf{B}}(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)) \leq \sum_{u \in \mathcal{V}_i^{\mathsf{B}}(\Pi)} P_i(u) \cdot \mathrm{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle), \tag{55}$$

and that

$$\sum_{u \in \mathcal{V}_i(\Pi)} P_i(u) \cdot \mathrm{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle) \leq 2 \cdot \mathrm{SD}(\langle \Pi \rangle, \langle \Pi' \rangle). \tag{56}$$

Plugging Equations (54) to (56) into Equation (53) completes the proof of Claim 4.11.

Proof of Equation (54): Let $u \in \mathcal{V}_i^{\mathsf{A}}(\Pi)$. By the definition of f, and since u is under A's control, it follows that $\Pr[f(u) = \ell] = \langle \Pi_u \rangle(\ell)/\mathsf{val}(\Pi_u)$ if $\chi_\Pi(\ell) = 1$, and $\Pr[f(u) = \ell] = 0$ otherwise. Since Π and Π' have the same control scheme, the same holds for $g(u)$ with respect to Π'. Let $\mathcal{S}'_u \subseteq \mathcal{L}_1(\Pi)$ be the set with $\mathrm{SD}(f(u), g(u)) = \sum_{\ell \in \mathcal{S}'_u} (\Pr[f(u) = \ell] - \Pr[g(u) = \ell]) = \sum_{\ell \in \mathcal{L}_1(\Pi) \setminus \mathcal{S}'_u} (\Pr[g(u) = \ell] - \Pr[f(u) = \ell])$.[47] Define $\mathcal{S}_u \subseteq \mathcal{L}_1(\Pi)$ as follows: if $\mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u)$, let $\mathcal{S}_u = \mathcal{S}'_u$; otherwise, let $\mathcal{S}_u = \mathcal{L}_1(\Pi) \setminus \mathcal{S}'_u$. It follows that

$$\begin{aligned}\sum_{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi)} P_i(u) \cdot \mathrm{SD}(f(u), g(u)) \leq & \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi): \\ \mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u) \geq \delta'}} P_i(u) \cdot \sum_{\ell \in \mathcal{S}_u} \left(\frac{\langle \Pi_u \rangle(\ell)}{\mathsf{val}(\Pi_u)} - \frac{\langle \Pi'_u \rangle(\ell)}{\mathsf{val}(\Pi'_u)}\right) \\ & + \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi): \\ \mathsf{val}(\Pi'_u) > \mathsf{val}(\Pi_u) \geq \delta'}} P_i(u) \cdot \sum_{\ell \in \mathcal{S}_u} \left(\frac{\langle \Pi'_u \rangle(\ell)}{\mathsf{val}(\Pi'_u)} - \frac{\langle \Pi_u \rangle(\ell)}{\mathsf{val}(\Pi_u)}\right) \\ & + \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi): \\ \mathsf{val}(\Pi_u) < \delta' \vee \mathsf{val}(\Pi'_u) < \delta'}} P_i(u).\end{aligned} \tag{57}$$

Assume $\mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u)$. The definition of $\mathcal{S}_u$ implies that $\langle \Pi_u \rangle(\ell)/\mathsf{val}(\Pi_u) \geq \langle \Pi'_u \rangle(\ell)/\mathsf{val}(\Pi'_u)$ for every $\ell \in \mathcal{S}_u$. But since $\mathsf{val}(\Pi_u)/\mathsf{val}(\Pi'_u) \geq 1$, the latter yields that $\langle \Pi_u \rangle(\ell) \geq \langle \Pi'_u \rangle(\ell)$ for every

[47] Note that it must be the case that $\mathcal{S}'_u \subseteq \mathcal{L}_1(\Pi)$, since $\Pr[f(u) = \ell] = \Pr[g(u) = \ell] = 0$, for every ℓ with $\chi_\Pi(\ell) = 0$, which follows from the assumption that $\chi_\Pi \equiv \chi_{\Pi'}$.

$\ell \in \mathcal{S}_u$. Using this observation, we bound the first summand in the right-hand side of Equation (57):

$$\begin{aligned}
&\sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u) \geq \delta'}} P_i(u) \cdot \sum_{\ell \in \mathcal{S}_u} \left(\frac{\langle \Pi_u \rangle(\ell)}{\mathsf{val}(\Pi_u)} - \frac{\langle \Pi'_u \rangle(\ell)}{\mathsf{val}(\Pi'_u)} \right) \qquad (58)\\
&\leq \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u) \geq \delta'}} \frac{P_i(u)}{\mathsf{val}(\Pi')} \cdot \sum_{\ell \in \mathcal{S}_u} \left(\langle \Pi_u \rangle(\ell) - \langle \Pi'_u \rangle(\ell) \right)\\
&\leq \frac{1}{\delta'} \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u) \geq \delta'}} P_i(u) \cdot \sum_{\ell \in \mathcal{S}_u} \left(\langle \Pi_u \rangle(\ell) - \langle \Pi'_u \rangle(\ell) \right)\\
&\leq \frac{1}{\delta'} \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi_u) \geq \mathsf{val}(\Pi'_u) \geq \delta'}} P_i(u) \cdot \mathsf{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle),
\end{aligned}$$

where the second inequality follows since $\sum_{\ell \in \mathcal{S}_u} (\langle \Pi_u \rangle(\ell) - \langle \Pi'_u \rangle(\ell)) \geq 0$, as argued above. With similar calculations, and using the symmetry of statistical distance, we bound the second summand in the right-hand side of Equation (57):

$$\begin{aligned}
&\sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi'_u) \geq \mathsf{val}(\Pi_u) \geq \delta'}} P_i(u) \cdot \sum_{\ell \in \mathcal{S}_u} \left(\frac{\langle \Pi'_u \rangle(\ell)}{\mathsf{val}(\Pi'_u)} - \frac{\langle \Pi_u \rangle(\ell)}{\mathsf{val}(\Pi_u)} \right) \qquad (59)\\
&\leq \frac{1}{\delta'} \sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi'_u) \geq \mathsf{val}(\Pi_u) \geq \delta'}} P_i(u) \cdot \mathsf{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle).
\end{aligned}$$

Finally, to bound the third summand in the right-hand side of Equation (57), we note that it sums over (not all) $u \in \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}}$. Since P_i simply samples a random partial transcript from Π, it follows that

$$\sum_{\substack{u \in \mathcal{V}_i^{\mathsf{A}}(\Pi):\\ \mathsf{val}(\Pi_u) < \delta' \vee \mathsf{val}(\Pi'_u) < \delta'}} P_i(u) \leq \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta',\mathsf{C}} \right) \right]. \qquad (60)$$

Plugging Equations (58) to (60) into Equation (57) yields Equation (54).

Proof of Equation (55): Since it is the right-hand party who controls u in Π and in Π', it follows that $\mathsf{SD}(f(u), g(u)) = \mathsf{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle)$, and Equation (55) follows.

Proof of Equation (56): Using the definition of P_i, we can write

$$\begin{aligned}
&\sum_{u \in \mathcal{V}_i(\Pi)} P_i(u) \cdot \mathsf{SD}(\langle \Pi_u \rangle, \langle \Pi'_u \rangle)\\
&= \sum_{u \in \mathcal{V}_i(\Pi)} \mathsf{v}_{\Pi}(u) \cdot \frac{1}{2} \sum_{\ell \in \mathcal{L}(\Pi_u)} \left| \mathsf{v}_{\Pi_u}(\ell) - \mathsf{v}_{\Pi'_u}(\ell) \right|\\
&= \frac{1}{2} \sum_{\ell \in \mathcal{L}(\Pi)} \left| \mathsf{v}_{\Pi}(\ell_{1,\ldots,i-1}) \cdot \mathsf{v}_{\Pi_{\ell_{1,\ldots,i-1}}}(\ell) - \mathsf{v}_{\Pi}(\ell_{1,\ldots,i-1}) \cdot \mathsf{v}_{\Pi'_{\ell_{1,\ldots,i-1}}}(\ell) \right|\\
&= \mathsf{SD}(\langle \Pi \rangle, \langle \Pi'' \rangle),
\end{aligned}$$

for $\langle \Pi'' \rangle(\ell) := \mathsf{v}_{\Pi}(\ell_{1,\ldots,i-1}) \cdot \mathsf{v}_{\Pi'_{\ell_{1,\ldots,i-1}}}(\ell)$.

We prove that $\mathrm{SD}(\langle \Pi' \rangle, \langle \Pi'' \rangle) \le \mathrm{SD}(\langle \Pi' \rangle, \langle \Pi \rangle)$, and Equation (56) follows from the triangle inequality. Let h be the random function that, given $\ell \in \mathcal{L}(\Pi)$, returns $\ell' \leftarrow \langle \Pi'_{\ell_{1,\ldots,i-1}} \rangle$. Therefore, $h(\langle \Pi' \rangle) \equiv \langle \Pi' \rangle$ and $h(\langle \Pi \rangle) \equiv \langle \Pi'' \rangle$, and this completes the proof.

This completes the proof of Equations (54) to (56), and thus the proof of Claim 4.11. □

4.1.3 The Success Probability of $\mathsf{A}_\Pi^{(1,\xi,\delta)}$*—The "Ideal to Real" Reduction.* Consider an execution of $(\mathsf{A}^{(1,\xi,\delta)}, \mathsf{B})$. Such an execution asks the approximated biased continuator $\mathsf{BiasedCont}^{\xi,\delta}$ for continuations of transcripts under A's control, leading to 1-leaves. Hence, as long as this execution generates neither low-value transcripts under A's control nor unbalanced transcripts, we expect the approximated biased-continuation attacker to do almost as well as its ideal variant. This is formally put in the next lemma.

Lemma 4.12. *Let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be an m-round protocol and let* $\delta \in (0, \frac{1}{2}]$*. Then*

$$SD\left(\left\langle \mathsf{A}_\Pi^{(1)}, \mathsf{B} \right\rangle, \left\langle \mathsf{A}_\Pi^{(1,\xi,\delta)}, \mathsf{B} \right\rangle\right) \le m \cdot \gamma \cdot \left(2\xi + \Pr_{\langle \mathsf{A},\mathsf{B} \rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}})\right]\right) + \Pr_{\left\langle \mathsf{A}_\Pi^{(1)},\mathsf{B}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^{\gamma}\right)\right]$$

for every $\gamma \ge 1$ *and* $\xi > 0$.

Proof. We use Lemma 2.17. For function ϕ, let H^ϕ be an algorithm that outputs the transcript of a random execution of $(\mathsf{A}_\Pi^{(1)}, \mathsf{B})$ in which $\mathsf{A}_\Pi^{(1)}$'s calls to $\mathsf{BiasedCont}_\Pi$ are sent to ϕ instead.[48] Let f and g be the (random) functions $\mathsf{BiasedCont}_\Pi$ and $\mathsf{BiasedCont}_\Pi^{\xi,\delta}$, respectively, letting also $f(\perp) = g(\perp) = \perp$. By construction, it holds that

$$\mathrm{SD}\left(\left\langle \mathsf{A}_\Pi^{(1)}, \mathsf{B} \right\rangle, \left\langle \mathsf{A}_\Pi^{(1,\xi,\delta)}, \mathsf{B} \right\rangle\right) = \mathrm{SD}\left(\mathsf{H}^f, \mathsf{H}^g\right). \tag{61}$$

For $i \in [m]$, let P'_i be the distribution of the ith node under A's control in a random execution of Π, taking the value $\perp$ if no such node exists, and let $P_i = (P'_i, 1)$, with $(\perp, 1) = \perp$. By definition,

$$\begin{aligned} \mathrm{E}_{q \leftarrow P_i}[\mathrm{SD}(f(q), g(q))] &= \mathrm{E}_{q \leftarrow P_i}\left[\mathrm{SD}(\mathsf{BiasedCont}_\Pi(q), \mathsf{BiasedCont}_\Pi^{\xi,\delta}(q)) \cdot 1_{\neg\perp}(q)\right] \\ &\le 2\xi + \Pr_{\langle \Pi \rangle}\left[\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}})\right], \end{aligned} \tag{62}$$

letting the indicator $1_{\neg\perp}(q)$ take the value one if $q \ne \perp$, and zero otherwise.

Let Q_i denote the ith query to f in a random execution of H^f, taking the value $\perp$ if no such query exists, and let $Q = (Q_1, \ldots, Q_m)$. By definition,

$$\Pr_{(q_1,\ldots,q_m) \leftarrow Q}[\exists i \in [m] : q_i \ne \perp \wedge Q_i(q_i) > \gamma \cdot P_i(q_i)] = \Pr_{\left\langle \mathsf{A}_\Pi^{(1)},\mathsf{B}\right\rangle}\left[\mathsf{desc}\left(\mathcal{U}\mathsf{nBal}_\Pi^{\gamma}\right)\right]. \tag{63}$$

Hence, the proof follows by Lemma 2.17, letting $k := m$, $a := 2\xi + \Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{A}})]$, $\lambda := \gamma$ and $b := \Pr_{\langle \mathsf{A}_\Pi^{(1)},\mathsf{B}\rangle}[\mathsf{desc}(\mathcal{U}\mathsf{nBal}_\Pi^{\gamma})]$. □

Our use of Lemma 4.12 is via the following lemma that states that the approximated biased-continuation attacker successfully biases protocols in which the probability of hitting A-controlled low-value nodes is small.

[48] Note that H is not the same as Algorithm 4.10 defined in the proof of the robustness lemma (Lemma 4.9). There we considered two different underlying protocols and needed to also argue about the different actions the honest (i.e., nonattacked) parties took. Here, we have only one underlying protocol and thus care only about the calls the attacked party makes.

Lemma 4.13. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an m-round protocol, let $\delta \in (0, \frac{1}{2}]$, and let $c = c(\delta)$ be according to Lemma 4.7; then*

$$SD\Big(\Big\langle \mathsf{A}_{\Pi}^{(1)}, \mathsf{B}\Big\rangle, \Big\langle \mathsf{A}_{\Pi}^{(1,\xi,\delta')}, \mathsf{B}\Big\rangle\Big) \leq 2 \cdot m \cdot \gamma \cdot \Big(\xi + \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\Big[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}})\Big]\Big) + \frac{2}{\gamma^c}$$

for any $\delta' \geq \delta$, $\xi > 0$, and $\gamma > 1$.

Proof. Follows by plugging Lemma 4.8 into Lemma 4.12. □

4.1.4 Bounding the Probability of Hitting Low-Density Sets. Our final step before proving Lemmas 4.4 and 4.5 is to show that the recursive ideal biased-continuation attacker does not increase the probability of hitting any set by much. This is a generalization of Lemma 4.8 to arbitrary sets of nodes (i.e., not only unbalanced) and to the recursive version of the ideal biased-continuation attacker.

Lemma 4.8 considered unbalanced nodes to be those that the probability of hitting them in the protocol in which the (nonrecursive) biased-continuation attacker takes the role of A is γ-times higher than in the original protocol. When extending Lemma 4.8 to the recursive version of the attacker, we take different degrees of "unbalancedness" for every level of the recursion. Specifically, we will (implicitly) define unbalanced nodes for the ith level of the recursion to be those nodes that the probability of hitting them in the protocol in which the ith-level recursive attacker takes the role of A is γ_i-times higher than in the protocol in which the $(i-1)$'th-level recursive attacker takes the role of A. The freedom to choose different degrees of "unbalanceness" for different levels of the recursion will be crucial when arguing that (a similar attack to) the biased-continuation attack can be can implemented efficiently assuming the inexistence of OWFs.

Lemma 4.14. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol, let $\delta \in (0, \frac{1}{2}]$, and let $c = c(\delta)$ be according to Lemma 4.7. Then, for any $\delta' \geq \delta$, every $k \in \mathbb{N}$, any $(\gamma_1, \ldots, \gamma_k) \in (1, \infty)^k$, and every $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, it holds that*

$$\Pr_{\big\langle \mathsf{A}_{\Pi}^{(k)}, \mathsf{B}\big\rangle}\Big[\mathsf{desc}\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big)\Big] \leq \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\Big[\mathsf{desc}\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big)\Big] \cdot \prod_{i=1}^{k} \gamma_i$$
$$+ 2 \cdot \sum_{i=1}^{k} \frac{\cdot \prod_{j=i+1}^{k} \gamma_j}{\gamma_i^c}.$$

To prove Lemma 4.14, we will use the next claim.

Claim 4.15. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol, let $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, let $\delta \in (0, \frac{1}{2}]$, and let $c = c(\delta)$ from Lemma 4.7. Then, for every $\delta' \geq \delta$ and $\gamma > 1$, it holds that*

$$\Pr_{\big\langle \mathsf{A}_{\Pi}^{(1)}, \mathsf{B}\big\rangle}\Big[\mathsf{desc}\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big)\Big] \leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\Big[\mathsf{desc}\Big(\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big) \setminus \mathsf{desc}\Big(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}\Big)\Big)\Big]$$
$$+ \frac{2}{\gamma^c}.$$

Proof. Fix $\delta' \geq \delta$ and $\gamma > 1$. Applying Proposition 2.3 with respect to $\mathcal{A} = \mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}$, $\mathcal{B} = \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}$, and $C = \mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}$ yields that

$$\begin{aligned} &\mathsf{desc}\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big) \qquad (64) \\ &\subseteq \mathsf{desc}\Big(\Big(\mathcal{S} \cup \mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big) \setminus \mathsf{desc}\Big(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma}\Big)\Big) \cup \mathsf{desc}\Big(\mathcal{U}\mathsf{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathsf{desc}}\Big(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}}\Big)\Big). \end{aligned}$$

It follows that

$$\begin{aligned}\Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}[\mathrm{desc}(\mathcal{S})] &\leq \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathrm{desc}\left(\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right) \setminus \mathrm{desc}\left(\mathcal{U}\mathrm{nBal}_{\Pi}^{\gamma}\right)\right)\right] \\ &\quad + \Pr_{\langle \mathsf{A}^{(1)},\mathsf{B}\rangle}\left[\mathrm{desc}\left(\mathcal{U}\mathrm{nBal}_{\Pi}^{\gamma} \setminus \overline{\mathrm{desc}}\left(\mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right)\right] \\ &\leq \gamma \cdot \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathrm{desc}\left(\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right) \setminus \mathrm{desc}\left(\mathcal{U}\mathrm{nBal}_{\Pi}^{\gamma}\right)\right)\right] + \frac{2}{\gamma^c},\end{aligned}$$

where the first inequality follows from Equation (64) and the second inequality follows from the definition of $\mathcal{U}\mathrm{nBal}_{\Pi}^{\gamma}$ (Definition 4.6) and Lemma 4.7. □

We are now ready to prove Lemma 4.14.

Proof of Lemma 4.14. Fix $\delta' \geq \delta$ and $(\gamma_1, \ldots, \gamma_k) \in (1, \infty)^k$. The proof is by induction on k. For $k = 0$, the proof follows immediately from definition.

Assume the lemma holds for $k - 1$; we prove it for k. For $i \in (k - 1)$, let $\Pi^{(i)} = (\mathsf{A}_{\Pi}^{(i)}, \mathsf{B})$. It is easy to verify that when the ideal biased-continuation attacker takes the role of A in the protocol and tries to bias the outcome toward 1, the value of every node cannot decrease. Namely, it holds that $\mathcal{S}\mathrm{mall}_{\Pi^{(i)}}^{\delta',\mathsf{A}} \subseteq \mathcal{S}\mathrm{mall}_{\Pi^{(i-1)}}^{\delta',\mathsf{A}}$ for every $i \in [k - 1]$, and thus $\mathcal{S}\mathrm{mall}_{\Pi^{(k-1)}}^{\delta',\mathsf{A}} \subseteq \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}$. Applying Claim 4.15 with respect to the protocol $\Pi^{(k-1)}$, set $\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}$, and $\gamma = \gamma_k$ yields that

$$\begin{aligned}&\Pr_{\left\langle \mathsf{A}_{\Pi^{(k-1)}}^{(1)},\mathsf{B}\right\rangle}\left[\mathrm{desc}\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] \\ &\quad\leq \gamma_k \cdot \Pr_{\langle \Pi^{(k-1)}\rangle}\left[\mathrm{desc}\left(\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}} \cup \mathcal{S}\mathrm{mall}_{\Pi^{(k-1)}}^{\delta',\mathsf{A}}\right) \setminus \mathrm{desc}\left(\mathcal{U}\mathrm{nBal}_{\Pi^{(k-1)}}^{\gamma_k}\right)\right)\right] + \frac{2}{\gamma_k^c} \\ &\quad\leq \gamma_k \cdot \Pr_{\langle \Pi^{(k-1)}\rangle}\left[\mathrm{desc}\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] + \frac{2}{\gamma_k^c}.\end{aligned} \tag{65}$$

Equation (65) together with the induction hypothesis now yields that

$$\begin{aligned}&\Pr_{\left\langle \mathsf{A}_{\Pi^{(k-1)}}^{(1)},\mathsf{B}\right\rangle}\left[\mathrm{desc}\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] \\ &\quad\leq \gamma_k\left(\Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathrm{desc}\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] \cdot \prod_{i=1}^{k-1} \gamma_i + 2 \cdot \sum_{i=1}^{k-1} \frac{\cdot \prod_{j=i+1}^{k-1} \gamma_j}{\gamma_i^c}\right) + \frac{2}{\gamma_k^c} \\ &\quad= \Pr_{\langle \mathsf{A},\mathsf{B}\rangle}\left[\mathrm{desc}\left(\mathcal{S} \cup \mathcal{S}\mathrm{mall}_{\Pi}^{\delta',\mathsf{A}}\right)\right] \cdot \prod_{i=1}^{k} \gamma_i + 2 \cdot \sum_{i=1}^{k} \frac{\cdot \prod_{j=i+1}^{k} \gamma_j}{\gamma_i^c}.\end{aligned}$$

Noting that $(\mathsf{A}_{\Pi^{(k-1)}}^{(1)}, \mathsf{B}) = (\mathsf{A}_{\Pi}^{(k)}, \mathsf{B})$ concludes the proof. □

4.1.5 Proving Lemmas 4.4 and 4.5.

We are finally ready to prove Lemmas 4.4 and 4.5. These proofs rely on the next lemma, a slight generalization to Lemma 4.4.

Lemma 4.16. *For any $\delta \in (0, 1/4]$, there exists a constant $c = c(\delta)$ such that the following holds. Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a m-round protocol, and assume $\Pr_{\langle \Pi\rangle}[\mathrm{desc}(\mathcal{S}\mathrm{mall}_{\Pi}^{1.5\delta',\mathsf{A}})] \leq \alpha$ for some $\delta \leq \delta' \leq \frac{1}{4}$. Then, for every $\xi \in (0, 1)$, $k \in \mathbb{N}$, and $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k) \in (1, \infty)^k$, it holds that*

$$SD\left(\left\langle \mathsf{A}_{\Pi}^{(k)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_{\Pi}^{(k,\xi,\delta')}, \mathsf{B}\right\rangle\right) \leq k \cdot \frac{30^k \cdot m^k \cdot \prod_{i=1}^{k} \gamma_i}{\delta'^{2k}} \cdot (\alpha + \xi) \tag{66}$$

$$+\sum_{i=1}^{k} 2^{k-i+2} \cdot \frac{30^{k-i} \cdot m^{k-i} \cdot \prod_{j=i+1}^{k} \gamma_j}{\delta'^{2(k-i)} \cdot \gamma_i^c}. \tag{67}$$

Before proving this lemma, we use it to derive Lemmas 4.4 and 4.5.

Proving Lemma 4.4.

Proof of Lemma 4.4. Fix $\delta \in (0,1/4]$, $k \in \mathbb{N}$. Also fix $\delta' \in [\delta, 1/4]$ for which $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}})] \leq \alpha$. Furthermore, fix $\xi \in (0,1)$ and $\mu \in (0,1)$ and let $c = c(\delta)$ be the constant guaranteed by Lemma 4.16. We begin by defining a vector $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k) \in (1,\infty)^k$ with respect to the sum in Equation (67) that is less than μ. For $i \in [k]$, let

$$t_i := 2^{k-i+2} \cdot \frac{30^{k-i} \cdot m^{k-i} \cdot \prod_{j=i+1}^{k} \gamma_j}{\delta'^{2(k-i)} \cdot \gamma_i^c}. \tag{68}$$

The sum in Equation (67) can be now written as $\sum_{i=1}^{k} t_i$. We now define $\boldsymbol{\gamma}$ so that $t_i \leq \mu/2^i$ for every i, implying that $\sum_{i=1}^{k} t_i \leq \mu$. Let $\gamma_k := \lceil (4 \cdot 2^k/\mu)^{1/c} \rceil$. Note that

$$t_k = \frac{4}{\gamma_k^c} \leq \frac{\mu}{2^k}. \tag{69}$$

The value of $\gamma_{k-1}, \ldots, \gamma_1$ is set inductively. For $i \in [k-1]$, let

$$\gamma_i := \left\lceil \left(2^{k-i+2} \cdot \frac{30^{k-i} \cdot m^{k-i} \cdot \prod_{j=i+1}^{k} \gamma_j}{\delta'^{2(k-i)}} \cdot \frac{2^i}{\mu} \right)^{1/c} \right\rceil.$$

By construction, it holds that $\prod_{j=i+1}^{k} \gamma_j \in \mathrm{poly}(m, 1/\delta', 1/\mu)$, $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k) \in (1,\infty)^k$, and that $\sum_{i=1}^{k} t_i \leq \mu$. The proof is thus concluded by applying Lemma 4.16. □

Proving Lemma 4.5.

Proof of Lemma 4.5. Fix $\delta \in (0,1/4]$, $k \in \mathbb{N}$. Also fix $\delta' \in [\delta, 1/4]$ for which $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}})] \leq \alpha$. Let $c = c(\delta)$ be the constant guaranteed by Lemma 4.16. Set $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k) \in (1,\infty)^k$ in the same way it was set in the proof of Lemma 4.4 above. By assumption, it holds that $\Pr_{\langle\Pi\rangle}[\mathsf{desc}(\mathcal{F})] \leq \beta + \varepsilon$. Applying Lemma 4.14 yields that

$$\Pr_{\left\langle \mathsf{A}_{\Pi}^{(k)}, \mathsf{B} \right\rangle}[\mathsf{desc}(\mathcal{F})] \leq (\alpha + \beta + \varepsilon) \cdot \prod_{i=1}^{k} \gamma_i + 2 \cdot \sum_{i=1}^{k} \frac{\cdot \prod_{j=i+1}^{k} \gamma_j}{\gamma_i^c},$$

and Lemma 4.16 now yields that

$$\Pr_{\left\langle \mathsf{A}_{\Pi}^{(k,\delta',\xi)}, \mathsf{B} \right\rangle}[\mathsf{desc}(\mathcal{F})] \leq (\alpha + \beta + \varepsilon) \cdot \prod_{i=1}^{k} \gamma_i + 2 \cdot \sum_{i=1}^{k} \frac{\cdot \prod_{j=i+1}^{k} \gamma_j}{\gamma_i^c} \tag{70}$$

$$+ k \cdot \frac{30^k \cdot m^k \cdot \prod_{i=1}^{k} \gamma_i}{\delta'^{2k}} \cdot (\alpha + \xi) \tag{71}$$

$$+\sum_{i=1}^{k} 2^{k-i+2} \cdot \frac{30^{k-i} \cdot m^{k-i} \cdot \prod_{j=i+1}^{k} \gamma_j}{\delta'^{2(k-i)} \cdot \gamma_i^c}. \tag{72}$$

By the proof of Lemma 4.4 above, the terms in Equations (71) and (72) are at most $\phi_{k,\delta}^{\mathsf{It}}(\alpha, \xi, m, \delta', \mu)$. Moreover, the proof of Lemma 4.4 also yields that the term in Equation (72) is at most μ and that $\prod_{i=1}^{k} \gamma_i \in \mathrm{poly}(m, 1/\delta', 1/\mu)$. The proof is concluded by noting that the second term in the right-hand side of Equation (70) is bounded from above by that in Equation (72) and thus is also at most μ. □

Proving Lemma 4.16. Lemma 4.16 is proven by induction on k. The next lemma, which combines the results from the previous sections, will be useful to argue the induction step.

Lemma 4.17. *For every $\delta \in (0, 1/4]$, there exists a constant $c = c(\delta)$ such that the following holds. Let $\Pi = (\mathsf{A}, \mathsf{B})$ and $\Pi' = (\mathsf{C}, \mathsf{D})$ be two m-round protocols with the same control scheme, and assume*

(1) $\chi_\Pi \equiv \chi_{\Pi'}$,
(2) $SD(\langle \Pi \rangle, \langle \Pi' \rangle) \le \beta$, and
(3) $\Pr_{\langle \Pi' \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi'}^{1.5\delta', \mathsf{C}})] \le \alpha$ for some $\delta \le \delta' \le \frac{1}{4}$.

Then, for every $\xi \in (0, 1)$ and $\gamma > 1$, it holds that

$$SD\left(\left\langle \mathsf{A}_\Pi^{(1,\xi,\delta')}, \mathsf{B} \right\rangle, \left\langle \mathsf{C}_{\Pi'}^{(1)}, \mathsf{D} \right\rangle\right) \le \frac{30 \cdot m \cdot \gamma}{\delta'^2} \cdot (\alpha + \xi + \beta) + \frac{4}{\gamma^c}.$$

Proof. Fix $\delta \in (0, 1/4]$ and let $c = c(\delta)$ be according to Lemma 4.7. Fix $\delta' \in [\delta, 1/4]$ for which $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta', \mathsf{A}})] \le \alpha$. Furthermore, fix $\xi \in (0, 1)$ and $\gamma > 1$.

The proof proceeds in two steps. First, apply Lemma 4.9 (robustness lemma) to show that after the (ideal) biased-continuation attacker takes the role of A and C in Π and Π', respectively, the leaf distributions of these protocols remain close. Second, apply Lemma 4.13 (ideal-to-approximated biased-continuation attacker) to show that by replacing the attacker of the left-hand party in Π with its approximated variant, the leaf distributions of these protocols remain close.

In order to apply Lemma 4.9, we first need to bound $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta', \mathsf{C}})]$. Let $\mathcal{F} = \mathsf{frnt}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta', \mathsf{C}})$, let $\mathcal{F}_1 = \{u \in \mathcal{F} : \mathsf{val}((\Pi')_u) \ge 1.5\delta'\}$, and let $\mathcal{F}_2 = \{u \in \mathcal{F} : \mathsf{val}((\Pi')_u) < 1.5\delta'\}$. Since $\mathcal{F} \subseteq \mathcal{F}_1 \bigcup \mathcal{F}_2$, it suffices to bound $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}_1)]$ and $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}_2)]$, which we do separately.

Bounding $\mathcal{F}_1$: Nodes in $\mathcal{F}_1$ must have a small value in Π but a large value in Π'. Since $\langle \Pi \rangle$ and $\langle \Pi' \rangle$ are close, the probability of reaching such nodes is small.

Formally, since every node in $\mathcal{F}_1$ must belong to $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}}$, it follows that $\Pr_{\langle \Pi \rangle}[\mathcal{L}_1(\Pi) \mid \mathsf{desc}(\mathcal{F}_1)] \le \delta'$. Assumption (1) of the lemma and the definition of $\mathcal{F}_1$ yield, however, that $\Pr_{\langle \Pi' \rangle}[\mathcal{L}(\Pi) \mid \mathsf{desc}(\mathcal{F}_1)] \ge 1.5\delta'$. It follows from Proposition 2.8 that

$$\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}_1)] \le \beta \cdot \frac{1 + 1.5\delta'}{0.5\delta'} \le \frac{4\beta}{\delta'}.$$

The last inequality holds since, by assumption, $\delta' \le 1/4$.

Bounding $\mathcal{F}_2$: The definition of $\mathcal{F}_2$, the assumption that Π and Π' have the same control scheme, and assumption (3) yield that $\Pr_{\langle \Pi' \rangle}[\mathsf{desc}(\mathcal{F}_2)] \le \alpha$. Hence, the assumption that $\mathrm{SD}(\langle \Pi \rangle, \langle \Pi' \rangle) \le \beta$ (assumption (2) of the lemma) yields that $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}_2)] \le \alpha + \beta$.

Combining the two bounds, it follows that $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta', \mathsf{C}})] \le 5\beta/\delta' + \alpha$. We can apply Lemma 4.9 and derive

$$\mathrm{SD}\left(\left\langle \mathsf{A}_\Pi^{(1)}, \mathsf{B} \right\rangle, \left\langle \mathsf{C}_{\Pi'}^{(1)}, \mathsf{D} \right\rangle\right) \le \frac{3 \cdot m \cdot \gamma}{\delta'} \cdot \left(\beta + \frac{5\beta}{\delta'} + \alpha\right) + \frac{2}{\gamma^c}. \tag{73}$$

The next step is to apply Lemma 4.13. To do so, we need to bound $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}})]$, but since it is clear that $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}})] \le \Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta', \mathsf{A}} \cup \mathcal{S}\mathsf{mall}_{\Pi'}^{\delta', \mathsf{C}})]$, it follows that

$\Pr_{\langle \Pi \rangle}[\mathrm{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{\delta',\mathsf{A}})] \le 5\beta/\delta' + \alpha$. Applying Lemma 4.13, we derive

$$\mathrm{SD}\left(\left\langle \mathsf{A}_{\Pi}^{(1)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_{\Pi}^{(1,\xi,\delta')}, \mathsf{B}\right\rangle\right) \le 2 \cdot m \cdot \gamma \cdot \left(\xi + \frac{5\beta}{\delta'} + \alpha\right) + \frac{2}{\gamma^c}. \tag{74}$$

Finally, applying the triangle inequality of statistical distance to Equations (73) and (74) completes the proof of Lemma 4.17. □

The proof of Lemma 4.16 now follows straightforward calculations.

Proof of Lemma 4.16. Fix $\delta \in (0, 1/4]$ and let $c = c(\delta)$ be according to Lemma 4.17. Fix $\delta' \in [\delta, 1/4]$ for which $\Pr_{\langle \Pi \rangle}[\mathrm{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}})] \le \alpha$. Furthermore, fix $\xi \in (0, 1)$.

The proof is by induction on k. For $k = 0$, the proof follows immediately from the definition.

Fix $k \in \mathbb{N}$ and let $(\gamma_1, \ldots, \gamma_k) \in (1, \infty)^k$. Assume the lemma holds for $k - 1$; we prove it for k by applying Lemma 4.17. For $i \in (k)$, let $\Pi_1^{(i)} = (\mathsf{A}_{\Pi}^{(i)}, \mathsf{B})$ and let $\Pi_2^{(i)} = (\mathsf{A}_{\Pi}^{(i,\xi,\delta')}, \mathsf{B})$. Using this notation, we can write $\Pi_1^{(k)} = (\mathsf{A}_{\Pi_1^{(k-1)}}^{(1)}, \mathsf{B})$ and $\Pi_2^{(k)} = (\mathsf{A}_{\Pi_2^{(k-1)}}^{(1,\xi,\delta')}, \mathsf{B})$. Hence,

$$\mathrm{SD}\left(\left\langle \mathsf{A}_{\Pi}^{(k)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_{\Pi}^{(k,\xi,\delta')}, \mathsf{B}\right\rangle\right) = \mathrm{SD}\left(\left\langle \mathsf{A}_{\Pi_1^{(k-1)}}^{(1)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_{\Pi_2^{(k-1)}}^{(1,\xi,\delta')}, \mathsf{B}\right\rangle\right). \tag{75}$$

We would like to apply Lemma 4.17 with respect to $\Pi_1^{(k-1)}$ and $\Pi_2^{(k-1)}$. Indeed, these protocols share the same control scheme and common output function χ, and the induction hypothesis gives us a bound for $\mathrm{SD}(\langle \Pi_1^{(k-1)} \rangle, \langle \Pi_2^{(k-1)} \rangle)$. It remains to bound $\Pr_{\langle \Pi_1^{(k-1)} \rangle}[\mathrm{desc}(\mathcal{S}\mathsf{mall}_{\Pi_1^{(k-1)}}^{1.5\delta',\mathsf{A}})]$.

As we argued before,[49] it is easy to verify that when the ideal biased-continuation attacker takes the role of A in the protocol and tries to bias the outcome toward 1, the value of every node cannot decrease. Namely, it holds that $\mathcal{S}\mathsf{mall}_{\Pi_1^{(i)}}^{1.5\delta',\mathsf{A}} \subseteq \mathcal{S}\mathsf{mall}_{\Pi_1^{(i-1)}}^{1.5\delta',\mathsf{A}}$ for every $i \in [k-1]$, and thus $\mathcal{S}\mathsf{mall}_{\Pi_1^{(k-1)}}^{1.5\delta',\mathsf{A}} \subseteq \mathcal{S}\mathsf{mall}_{\Pi_1}^{1.5\delta',\mathsf{A}} = \mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}}$. It holds that

$$\begin{aligned} \Pr_{\langle \Pi_1^{(k-1)} \rangle}\left[\mathrm{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi_1^{(k-1)}}^{1.5\delta',\mathsf{A}}\right)\right] &\le \Pr_{\langle \Pi_1^{(k-1)} \rangle}\left[\mathrm{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}}\right)\right] \\ &\le \Pr_{\langle \Pi \rangle}\left[\mathrm{desc}\left(\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}}\right)\right] \cdot \prod_{i=1}^{k-1} \gamma_i + 2 \cdot \sum_{i=1}^{k-1} \frac{\cdot \prod_{j=i+1}^{k-1} \gamma_j}{\gamma_i^c} \\ &\le \alpha \cdot \prod_{i=1}^{k-1} \gamma_i + 2 \cdot \sum_{i=1}^{k-1} \frac{\cdot \prod_{j=i+1}^{k-1} \gamma_j}{\gamma_i^c}. \end{aligned} \tag{76}$$

The second inequality follows from applying Lemma 4.14 with respect to $1.5\delta'$ and the set $\mathcal{S}\mathsf{mall}_{\Pi}^{1.5\delta',\mathsf{A}}$. By the induction hypothesis and Lemma 4.17 applied to $\Pi_1^{(k-1)}$ and $\Pi_2^{(k-1)}$ with respect

[49] We used the same argument in the proof of Lemma 4.14.

to γ_k, it holds that

$$\begin{aligned}
&\mathrm{SD}\left(\left\langle \mathsf{A}_\Pi^{(k)}, \mathsf{B}\right\rangle, \left\langle \mathsf{A}_\Pi^{(k,\xi,\delta')}, \mathsf{B}\right\rangle\right) \\
&\quad \leq \frac{30 \cdot m \cdot \gamma_k}{\delta'^2} \cdot \Bigg((k-1) \cdot \frac{30^{k-1} \cdot m^{k-1} \cdot \prod_{i=1}^{k-1} \gamma_i}{\delta'^{2(k-1)}} \cdot (\xi + \alpha) \\
&\qquad\qquad + \sum_{i=1}^{k-1} 2^{k-i+1} \cdot \frac{30^{k-1-i} \cdot m^{k-1-i} \cdot \prod_{j=i+1}^{k-1} \gamma_j}{\delta'^{2(k-1-i)} \cdot \gamma_i^c} \\
&\qquad\qquad + \alpha \cdot \prod_{i=1}^{k-1} \gamma_i + 2 \cdot \sum_{i=1}^{k-1} \frac{\cdot \prod_{j=i+1}^{k-1} \gamma_j}{\gamma_i^c} + \xi \Bigg) + \frac{4}{\gamma_k^c} \\
&\quad = \frac{30 \cdot m \cdot \gamma_k}{\delta'^2} \cdot \left((k-1) \cdot \frac{30^{k-1} \cdot m^{k-1} \cdot \prod_{i=1}^{k-1} \gamma_i}{\delta'^{2(k-1)}} \cdot (\xi + \alpha) + \alpha \cdot \prod_{i=1}^{k-1} \gamma_i + \xi \right) \\
&\qquad + \frac{30 \cdot m \cdot \gamma_k}{\delta'^2} \cdot \left(\sum_{i=1}^{k-1} 2^{k-i+1} \cdot \frac{30^{k-1-i} \cdot m^{k-1-i} \cdot \prod_{j=i+1}^{k-1} \gamma_j}{\delta'^{2(k-1-i)} \cdot \gamma_i^c} + 2 \cdot \sum_{i=1}^{k-1} \frac{\cdot \prod_{j=i+1}^{k-1} \gamma_j}{\gamma_i^c} \right) + \frac{4}{\gamma_k^c}.
\end{aligned}$$

The induction proof now follows by grouping together the summands in the parentheses. This concludes the proof of Lemma 4.24. □

4.2 Attacking Pruned Protocols

In Section 4.1, we showed that if in a protocol $\Pi = (\mathsf{A}, \mathsf{B})$ the probability to visit A-controlled low-value nodes is small, then the recursive approximated biased-continuation attacker (taking the role of A) biases the outcome of the protocol toward one almost as well as its ideal variant does (a similar fact holds for the attacker taking the role of B, trying to bias the outcome of the protocol toward zero, and the probability to visit B-controlled high-value nodes is small). For some protocols, however, this probability might be arbitrarily large, so the analysis in Section 4.1 does not suffice to argue that the recursive approximated biased-continuation attacker successfully biases *any* protocol. In this section, we define the pruned variant of a protocol so that the probability of hitting A-controlled low-value nodes, as well as hitting B-controlled high-value nodes, is indeed small. Hence, Lemma 4.4 yields that the recursive approximated biased-continuation attacker successfully biases the pruned variant of any protocol. In Section 4.3, we exploit the above for attacking *any* protocol by letting the attacker "pretend" it is attacking a pruned variant, rather than the original protocol.

We start with defining an ideal pruned variant of a protocol, in which there exist no A-controlled low-value nodes and B-controlled high-value nodes. This variant, however, might not be efficiently computed, even if OWFs do not exist. To cope with this efficiency issue, we consider an approximated variant of the pruned protocol in which such nodes might exist but the probability of hitting them is small. Finally, we apply the results from Section 4.1 to argue that the recursive approximated biased-continuation attacker biases the outcome of the approximately pruned variant of any protocol.

Pruned protocols. In the pruned variant of protocol $\Pi = (\mathsf{A}, \mathsf{B})$, the edge distribution remains intact, while the controlling scheme is changed, giving the control to B on low-value nodes and to A on high-value nodes.

Definition 4.18 (The Pruned Variant of a Protocol). Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an m-round protocol and let $\delta \in (0, \frac{1}{2})$. In the δ-pruned variant of Π, denoted by $\Pi^{[\delta]} = (\mathsf{A}_\Pi^{[\delta]}, \mathsf{B}_\Pi^{[\delta]})$, the parties follow the protocol Π, where $\mathsf{A}_\Pi^{[\delta]}$ and $\mathsf{B}_\Pi^{[\delta]}$ take the roles of A and B, respectively, with the following exception occurring the *first time* the protocol's transcript u is in $\mathcal{S}\mathsf{mall}_\Pi^\delta \cup \mathcal{L}\mathsf{arge}_\Pi^\delta$:

If $u \in \mathcal{L}\mathsf{arge}_\Pi^\delta$, set $\mathsf{C} = \mathsf{A}_\Pi^{[\delta]}$; otherwise, set $\mathsf{C} = \mathsf{B}_\Pi^{[\delta]}$. The party C takes control of the node u, samples a leaf $\ell \leftarrow \langle \Pi_u \rangle$, and then, bit by bit, sends $\ell_{|u|+1,\ldots,m}$ to the other party.

Namely, the first time the value of the protocol is close to either 1 or 0, the party interested in this value (i.e., $\mathsf{A}_\Pi^{[\delta]}$ for 1, and $\mathsf{B}_\Pi^{[\delta]}$ for 0) takes control and decides the outcome (without changing the value of the protocol). Hence, the protocol is effectively pruned at these nodes (each such node is effectively a parent of two leaves).

For every protocol Π, its pruned variant $\Pi^{[\delta]}$ is a well-defined protocol, so the analysis of Section 3 can be applied.[50] As mentioned above, the pruned variant of a protocol might *not* be efficiently computed, even if OWFs do not exist, so we move to consider an approximated variant of the pruned protocol.

Approximately pruned protocols. To define the approximated pruned protocols, we begin by defining two algorithms, both of which can be efficiently implemented assuming OWFs do not exist for an appropriate choice of parameters. The first algorithm samples an honest (i.e., unbiased) continuation of the protocol.

Definition 4.19 (Approximated Honest Continuation). Let Π be an m-round protocol, and let $\mathsf{HonCont}_\Pi$ be the algorithm that on node $u \in \mathcal{V}(\Pi)$ returns $\ell \leftarrow \langle \Pi_u \rangle$. Algorithm HC is a ξ-Honest-Continuator for Π if

$$\Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \mathsf{SD}(\mathsf{HC}(\ell_{1,\ldots,i}), \mathsf{HonCont}_\Pi(\ell_{1,\ldots,i})) > \xi\right] \le \xi.$$

Let $\mathsf{HonCont}_\Pi^\xi$ be an arbitrary (but fixed) ξ-honest-continuator for Π.

The second algorithm estimates the value of a given transcript (i.e., a node) of the protocol.

Definition 4.20 (Estimator). Let Π be an m-round protocol. A deterministic algorithm Est is a ξ-Estimator for Π if

$$\Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \left|\mathsf{Est}(\ell_{1,\ldots,i}) - \mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right| > \xi\right] \le \xi.$$

Let Est_Π^ξ be an arbitrary (but fixed) ξ-estimator for Π.

Using the above estimator, we define the approximated version of the low- and high-value nodes.

Definition 4.21 (Approximated Low-value and High-value Nodes). For protocol Π, $\delta \in (0, \frac{1}{2})$, and a deterministic real-value algorithm Est, let

- $\mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{Est}} = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{Est}(u) \le \delta\}$;
- $\mathcal{L}\mathsf{arge}_\Pi^{\delta,\mathsf{Est}} = \{u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \mathsf{Est}(u) \ge 1-\delta\}$.

For $\xi \in [0,1]$, let $\mathcal{S}\mathsf{mall}_\Pi^{\delta,\xi} = \mathcal{S}\mathsf{mall}_\Pi^{\delta,\mathsf{Est}_\Pi^\xi}$.

We can now define the approximately pruned protocol, which is the oracle variant of the ideal pruned protocol.

[50] Note that in the pruned protocol, the parties' turns might not alternate (i.e., the same party might send several consecutive bits), even if they do alternate in the original protocol. Rather, the protocol's control scheme (determining which party is active at a given point) is a function of the protocol's transcript and the original protocol's control scheme. Such schemes are consistent with the ones considered in the previous sections.

Definition 4.22 (The Approximately Pruned Variant of a Protocol). Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an m-round protocol, let $\delta \in (0, \frac{1}{2})$, let HC be an algorithm, and let Est be a deterministic real-value algorithm. The $(\delta, \mathsf{Est}, \mathsf{HC})$-approximately pruned variant of Π, denoted $\Pi^{[\delta, \mathsf{Est}, \mathsf{HC}]} = (\mathsf{A}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]}, \mathsf{B}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]})$, is defined as follows.

Control Scheme: The parties follow the control scheme of the protocol Π, where $\mathsf{A}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]}$ and $\mathsf{B}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]}$ take the roles of A and B, respectively, with the following exception occurring the *first time* the protocol's transcript u is in $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{Est}} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \mathsf{Est}}$: if $u \in \mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \mathsf{Est}}$ set $\mathsf{C} = \mathsf{A}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]}$; otherwise, set $\mathsf{C} = \mathsf{B}_{\Pi}^{[\delta, \mathsf{Est}, \mathsf{HC}]}$. The party C takes control of all nodes in $\operatorname{desc}(u)$ (i.e., nodes for which u is an ancestor).

Execution: For a protocol's transcript u and a party C who controls u, C sets $\ell = \mathsf{HC}(u)$ and sends $\ell_{|u|+1}$ to the other party.[51]

For $\delta \in (0, \frac{1}{2})$ and $\xi, \xi' \in [0, 1]$, let $\Pi^{[\delta, \xi, \xi']} = \Pi^{[\delta, \mathsf{Est}_{\Pi}^{\xi}, \mathsf{HonCont}_{\Pi}^{\xi'}]}$ and $\Pi^{[\delta, \xi]} = \Pi^{[\delta, \xi, \xi]}$, and the same notation is used for the parties of the pruned protocol.

Namely, in $\Pi^{[\delta, \xi]}$, the parties follow the control scheme of Π until reaching a node in $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \xi} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \xi}$ for the first time. Upon reaching such a node, the control moves to (and stays with) A if $u \in \mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \xi}$, or B if $u \in \mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \xi}$. The fact that the messages sent by the parties are determined by the answers of $\mathsf{HonCont}_{\Pi}^{\xi}$, instead of by their random coins, makes them *stateless* throughout the execution of the protocol. This fact will be crucial when implementing our final attacker.

Attacking approximately pruned protocols. We would like to argue about the success probability of the recursive approximated biased-continuation attacker when attacking approximately pruned protocols. To do so, we must first show that the probability of reaching A-controlled low-value nodes in such protocols is low. By definition, it is impossible to reach such nodes in the *ideal* pruned protocol. Thus, if the approximately pruned variant is indeed an approximation of the pruned variant of the protocol, we expect that probability of reaching A-controlled low-value nodes in this protocol will be low. Unfortunately, this does not necessarily hold. This is because the value of each node in both protocols might not be the same, and because the control scheme of these protocols might be different. It turns out that the bound for the above probability depends on the probability of the original protocol visiting nodes whose value is close to the pruning threshold, i.e., δ and $1 - \delta$.

Definition 4.23. For protocol Π, $\xi \in (0, 1)$, and $\delta \in (0, \frac{1}{2})$, let

$$\mathcal{B}\mathsf{order}_{\Pi}^{\delta, \xi} = \left\{ u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) : \begin{array}{r} \mathsf{val}(\Pi_u) \in (\delta - \xi, \delta + \xi] \\ \vee\ \mathsf{val}(\Pi_u) \in [1 - \delta - \xi, 1 - \delta + \xi) \end{array} \right\},$$

and let $\mathsf{border}_{\Pi}(\delta, \xi) = \Pr_{\langle \Pi \rangle}[\operatorname{desc}(\mathcal{B}\mathsf{order}_{\Pi}^{\delta, \xi})]$.

Namely, $\mathcal{B}\mathsf{order}_{\Pi}^{\delta, \xi}$ are those nodes that are ξ-close to the "border" between $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta}$ and the rest of the nodes. The intervals in the above definition are taken to be open on one side and closed on the other for technical reasons, and this fact is insignificant for the understanding of the definition.

We can now state the main result of this section—the recursive approximated biased-continuation attacker biases this approximated pruned protocol with similar success to that of the

[51] This happens to every transcript, even those that are not children of $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{Est}} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \mathsf{Est}}$.

recursive (ideal) biased-continuation attacker. Specifically, we have the following lemma, which is an application of Lemma 4.4 to the approximately pruned protocol.

Lemma 4.24. *Let $0 < \delta \le \delta' \le \frac{1}{4}$, let $\xi \in (0,1)$, and let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[2\delta',\xi]}$ be the $(2\delta',\xi)$-approximately pruned variant of a m-round protocol Π. Then,*

$$SD\left(\left\langle \mathsf{A}^{(k)}_{\widetilde{\Pi}}, \widetilde{\mathsf{B}}\right\rangle, \left\langle \mathsf{A}^{(k,\xi,\delta')}_{\widetilde{\Pi}}, \widetilde{\mathsf{B}}\right\rangle\right) \le \phi^{\mathsf{It}}_{k,\delta}(\mathsf{border}_{\Pi}(2\delta',\xi) + 12 \cdot m \cdot \xi/\delta', \xi, m, \delta', \mu),$$

for every $k \in \mathbb{N}$ and $\mu \in (0,1)$.[52]

The next lemma will also be useful ahead. It shows that if a set of nodes is reached with low probability in the original protocol, then the probability to reach the same set does not increase by much when the recursive approximated biased-continuation attacker attacks that approximately pruned variance of the protocol. This is an immediate application of Lemma 4.5 to the approximately pruned protocol.

Lemma 4.25. *Let $0 < \delta \le \delta' \le \frac{1}{4}$, let $\xi \in (0,1)$, and let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[2\delta',\xi]}$ be the $(2\delta',\xi)$-approximately pruned variant of an m-round protocol Π. Let $\mathcal{F}$ be a frontier with $\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F})] \le \beta$. Then*

$$\begin{aligned}\Pr_{\left\langle \mathsf{A}^{(k,\delta',\xi)}_{\widetilde{\Pi}}, \widetilde{\mathsf{B}}\right\rangle}[\mathsf{desc}(\mathcal{F})] \le\ & \phi^{\mathsf{Bal}}_{k,\delta}(\mathsf{border}_{\Pi}(2\delta',\xi) + 12 \cdot m \cdot \xi/\delta', \beta, 2 \cdot m \cdot \xi, m, \delta', \mu) \\ & + \phi^{\mathsf{It}}_{k,\delta}(\mathsf{border}_{\Pi}(2\delta',\xi) + 12 \cdot m \cdot \xi/\delta', \xi, m, \delta', \mu),\end{aligned}$$

for every $k \in \mathbb{N}$ and $\mu \in (0,1)$.[53]

Finally, in order for the above bounds to be useful, we need to show that $\mathsf{border}_{\Pi}(\delta,\xi)$—the probability in the original protocol of reaching nodes whose value is ξ-close to δ—is small. Unfortunately, given a protocol and a pruning threshold, this probability might be large. We argue, however, that if we allow a small deviation from the pruning threshold, this probability is small.

Lemma 4.26. *Let Π be an m-round protocol, let $\delta \in (0, \frac{1}{2}]$, and let $\xi \in (0,1)$. If $\xi \le \frac{\delta^2}{16m^2}$, then there exists $j \in \mathcal{J} := \{0, 1, \ldots, \lceil m/\sqrt{\xi} \rceil\}$ such that $\mathsf{border}_{\Pi}(\delta',\xi) \le m \cdot \sqrt{\xi}$ for $\delta' = \delta/2 + j \cdot 2\xi \in [\frac{\delta}{2}, \delta]$.*

The rest of this section is dedicated to proving the above lemmas. In Section 4.2.1, we show useful properties of approximately pruned protocols and use them to prove Lemmas 4.24 and 4.25. In Section 4.2.2, we prove Lemma 4.26.

4.2.1 Proving Lemmas 4.24 and 4.25.

Properties of approximately pruned protocols. In order to prove Lemmas 4.24 and 4.25, we need to bound the probability of hitting A-controlled low-value nodes with that of reaching nodes whose value is close to the pruning threshold in the original protocol (i.e., $\mathsf{border}_{\Pi}(\delta,\xi)$). The first step is to show that the approximately pruned protocol is close (in leaf distribution sense) to the original protocol.

Lemma 4.27. *Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an m-round protocol. Then*

$$SD\left(\langle \Pi \rangle, \left\langle \Pi^{[\delta,\xi]} \right\rangle\right) \le 2 \cdot m \cdot \xi$$

for every $\delta \in (0, 1/2]$ and $\xi \in (0,1)$.

[52] See Lemma 4.4 for the definition of $\phi^{\mathsf{It}}_{k,\delta}$.

[53] See Lemma 4.5 for the definition of $\phi^{\mathsf{Bal}}_{k,\delta}$.

The proof of Lemma 4.27 is a simple implication of the approximation guarantee of the honest continuator. Note that the leaf distributions of Π and $\Pi^{[\delta]}$ are identical, so the above lemma also shows that the leaf distributions of the ideal and approximated pruned protocols are close (i.e., that the latter is indeed an approximation to the former). Also note that the above bound does not depend on δ.

Proof. The proof is an application of Lemma 2.17. By definition, every message in $\Pi^{[\delta,\xi,0]}$ is set by calling a perfect honest continuator for Π. Thus, $\langle\Pi\rangle \equiv \langle\Pi^{[\delta,\xi,0]}\rangle$, and it suffices to bound $\mathrm{SD}(\langle\Pi^{[\delta,\xi,0]}\rangle, \langle\Pi^{[\delta,\xi]}\rangle = \langle\Pi^{[\delta,\xi,\xi]}\rangle)$, which we do by applying Lemma 2.17.

For a function ϕ, let H^{ϕ} be an algorithm that outputs the transcript of a random execution of $\Pi^{[\delta,\mathsf{Est}_{\Pi}^{\xi},\phi]}$. Let f and g be the (random) functions $\mathsf{HonCont}_{\Pi}$ and $\mathsf{HonCont}_{\Pi}^{\xi}$, respectively, and let $f(\perp) = g(\perp) = \perp$. By construction, it holds that

$$\mathrm{SD}\left(\left\langle\Pi^{[\delta,\xi,0]}\right\rangle, \left\langle\Pi^{[\delta,\xi,\xi]}\right\rangle\right) = \mathrm{SD}\left(\mathsf{H}^{f}, \mathsf{H}^{g}\right).$$

For $i \in [m]$, let P_i be the ith node in a random execution of Π (such a node consists of $i-1$ bits), and let $\mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i} = \{u \in \mathcal{V}(\Pi) : |u| = i-1 \wedge \mathrm{SD}(\mathsf{HonCont}_{\Pi}(u), \mathsf{HonCont}_{\Pi}^{\xi}(u)) > \xi\}$. By definition,

$$\begin{aligned}
&\Pr_{u\leftarrow P_i}\left[u \in \mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i}\right]\\
&\quad= \Pr_{\ell\leftarrow\langle\Pi\rangle}\left[\mathrm{SD}\left(\mathsf{HonCont}(\ell_{1,\ldots,i-1}), \mathsf{HonCont}_{\Pi}^{\xi}(\ell_{1,\ldots,i-1})\right) > \xi\right]\\
&\quad\leq \Pr_{\ell\leftarrow\langle\Pi\rangle}\left[\exists i \in [m] : \mathrm{SD}\left(\mathsf{HonCont}(\ell_{1,\ldots,i-1}), \mathsf{HonCont}_{\Pi}^{\xi}(\ell_{1,\ldots,i-1})\right) > \xi\right]\\
&\quad\leq \xi,
\end{aligned}$$

and thus,

$$\begin{aligned}
&\mathrm{E}_{u\leftarrow P_i}[\mathrm{SD}(f(u), g(u))]\\
&\quad= \mathrm{E}_{u\leftarrow P_i}\left[\mathrm{SD}\left(\mathsf{HonCont}_{\Pi}(u), \mathsf{HonCont}_{\Pi}^{\xi}(u)\right)\right]\\
&\quad= \Pr_{u\leftarrow P_i}\left[u \in \mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i}\right] \cdot \mathrm{E}_{u\leftarrow P_i}\left[\mathrm{SD}\left(\mathsf{HonCont}_{\Pi}(u), \mathsf{HonCont}_{\Pi}^{\xi}(u)\right) \;\middle|\; u \in \mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i}\right]\\
&\qquad+ \Pr_{u\leftarrow P_i}\left[u \notin \mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i}\right] \cdot \mathrm{E}_{u\leftarrow P_i}\left[\mathrm{SD}\left(\mathsf{HonCont}_{\Pi}(u), \mathsf{HonCont}_{\Pi}^{\xi}(u)\right) \;\middle|\; u \notin \mathcal{F}\mathsf{ailCont}_{\Pi}^{\xi,i}\right]\\
&\quad\leq \xi + \xi = 2\xi,
\end{aligned}$$

where the first equality follows since $P_i(\perp) = 0$.

Let Q_i denote the ith query to f in a random execution of H^{f} (note that by construction, such a query always exists) and let $Q = (Q_1, \ldots, Q_m)$. By definition, $Q_i \equiv P_i$, and thus

$$\Pr_{(q_1,\ldots,q_m)\leftarrow Q}[\exists i \in [m] : q_i \neq \perp \wedge Q_i(q_i) > P_i(q_i)] = 0.$$

The proof now follows by Lemma 2.17, letting $k = m$, $a = 2\xi$, $\lambda = 1$, and $b = 0$. □

We can now bound the probability of hitting A-controlled low-value nodes with that of reaching nodes whose value is close to the pruning threshold in the original protocol.

Lemma 4.28. *Let $\delta \in (0, 1/2)$, let $\varepsilon \in (0, \delta)$, let $\xi \in (0, 1)$, and let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[\delta,\xi]}$ be the (δ, ξ)-approximately pruned variant of an m-round protocol Π. Then*

$$\Pr_{\langle\widetilde{\Pi}\rangle}\left[\mathsf{desc}\left(\mathcal{S}\mathsf{mall}_{\widetilde{\Pi}}^{\delta-\varepsilon,\widetilde{\mathsf{A}}}\right)\right] \leq \mathsf{border}_{\Pi}(\delta, \xi) + \frac{6 \cdot m \cdot \xi}{\varepsilon}.$$

Proof of Lemma 4.28. The proof is an application of Lemma 4.27 and Proposition 2.8. Let $\mathcal{F}\mathsf{ailEst}_{\Pi}^{\xi} = \{u \in \mathcal{V}(\Pi) : |\mathsf{val}(\Pi_u) - \mathsf{Est}_{\Pi}^{\xi}(u)| > \xi\}$ and let $\mathcal{F} = \mathsf{frnt}(\mathcal{S}\mathsf{mall}_{\widetilde{\Pi}}^{\delta-\varepsilon,\widetilde{\mathsf{A}}}) \setminus$

$(\mathcal{B}\text{order}_{\Pi}^{\delta,\xi} \cup \mathcal{F}\text{ailEst}_{\Pi}^{\xi})$. It follows that

$$\Pr_{\langle\widetilde{\Pi}\rangle}\left[\text{desc}\left(\mathcal{S}\text{mall}_{\widetilde{\Pi}}^{\delta-\varepsilon,\widetilde{\mathsf{A}}}\right)\right] \le \Pr_{\langle\widetilde{\Pi}\rangle}\left[\text{desc}\left(\mathcal{B}\text{order}_{\Pi}^{\delta,\xi} \cup \mathcal{F}\text{ailEst}_{\Pi}^{\xi}\right)\right] + \Pr_{\langle\widetilde{\Pi}\rangle}[\text{desc}(\mathcal{F})]. \tag{77}$$

By Lemma 4.27, it holds that

$$\Pr_{\langle\widetilde{\Pi}\rangle}\left[\text{desc}\left(\mathcal{B}\text{order}_{\Pi}^{\delta,\xi} \cup \mathcal{F}\text{ailEst}_{\Pi}^{\xi}\right)\right] \le \text{border}_{\Pi}(\delta,\xi) + 3\cdot m\cdot\xi. \tag{78}$$

Let $u \in \mathcal{F}$. Since u is under $\widetilde{\mathsf{A}}$'s control, it holds that $\text{Est}_{\Pi}^{\xi}(u) > \delta$. Since $u \notin \mathcal{F}\text{ailEst}_{\Pi}^{\xi}$, it holds that $\text{val}(\Pi_u) > \delta - \xi$, and since $u \notin \mathcal{B}\text{order}_{\Pi}^{\delta,\xi}$, we have $\text{val}(\Pi_u) \ge \delta + \xi$. By definition, $\text{val}(\widetilde{\Pi}_u) \le \delta - \varepsilon$. Thus, $\Pr_{\langle\widetilde{\Pi}\rangle}[\mathcal{L}_1(\Pi) \mid \text{desc}(\mathcal{F})] \le \delta - \varepsilon$ and $\Pr_{\langle\Pi\rangle}[\mathcal{L}_1(\Pi) \mid \text{desc}(\mathcal{F})] \ge \delta + \xi$. Finally, by Lemma 4.27, it holds that $\text{SD}(\widetilde{\Pi},\Pi) \le 2\cdot m\cdot\xi$, and thus by Proposition 2.8 we have

$$\Pr_{\langle\widetilde{\Pi}\rangle}[\text{desc}(\mathcal{F})] \le 2\cdot m\cdot\xi\cdot\frac{1+\delta-\varepsilon}{\xi+\varepsilon} \le \frac{3\cdot m\cdot\xi}{\varepsilon}. \tag{79}$$

Plugging Equations (78) and (79) into Equation (77) completes the proof of the lemma. □

Proving Lemma 4.24.

Proof of Lemma 4.24. Applying Lemma 4.28 to $\widetilde{\Pi}$ and $\varepsilon = 0.5\delta'$ yields that

$$\Pr_{\langle\widetilde{\Pi}\rangle}\left[\text{desc}\left(\mathcal{S}\text{mall}_{\widetilde{\Pi}}^{1.5\delta',\widetilde{\mathsf{A}}}\right)\right] \le \text{border}_{\Pi}(2\delta',\xi) + \frac{12\cdot m\cdot\xi}{\delta'}. \tag{80}$$

The proof now immediately follows from Lemma 4.4. □

Proving Lemma 4.25.

Proof of Lemma 4.25. Immediately follows from plugging Lemma 4.27 and Equation (80) into Lemma 4.5. □

4.2.2 *Proving Lemma 4.26.*

Proof of Lemma 4.26. For $j \in \mathcal{J}$, let $\delta'(j) = \delta/2 + j\cdot 2\xi$. From the definition of $\mathcal{J}$, it is clear that $\delta'(j) \in [\frac{\delta}{2},\delta]$ for every $j \in \mathcal{J}$. Hence, it is left to argue that $\exists j \in \mathcal{J}$ such that $\text{border}_{\Pi}(\delta'(j),\xi) \le m\cdot\sqrt{\xi}$.

For $i \in [m]$, let $\mathcal{B}\text{order}_{\Pi}^{\delta,\xi,i} = \{u \in \mathcal{V}(\Pi) : u \in \mathcal{B}\text{order}_{\Pi}^{\delta,\xi} \wedge |u| = i-1\}$. It holds that

$$\begin{aligned}\Pr_{\langle\Pi\rangle}\left[\text{desc}\left(\mathcal{B}\text{order}_{\Pi}^{\delta,\xi}\right)\right] &\le \Pr_{\langle\Pi\rangle}\left[\text{desc}\left(\cup_{i\in[m]}\mathcal{B}\text{order}_{\Pi}^{\delta,\xi,i}\right)\right] \\ &\le \sum_{i=1}^{m}\Pr_{\langle\Pi\rangle}\left[\text{desc}\left(\mathcal{B}\text{order}_{\Pi}^{\delta,\xi,i}\right)\right].\end{aligned} \tag{81}$$

For every $i \in [m]$, let $\mathcal{N}(i) = \{j \in \mathcal{J} : \Pr_{\langle\Pi\rangle}[\text{desc}(\mathcal{B}\text{order}_{\Pi}^{\delta'(j),\xi,i})] > \sqrt{\xi}\}$ and let $\mathcal{N} = \cup_{i\in[m]}\mathcal{N}(i)$. We use the following claim (proven below). □

Claim 4.29. *It holds that $|\mathcal{N}(i)| < 1/\sqrt{\xi}$ for every $i \in [m]$.*

Claim 4.29 yields that $|\mathcal{N}| \le \sum_{i=1}^{m}|\mathcal{N}(i)| < \frac{m}{\sqrt{\xi}} < |\mathcal{J}|$. Thus, $\exists j \in \mathcal{J}$ such that $j \notin \mathcal{N}$. Set $\delta' = \delta'(j)$. It holds that $\Pr_{\langle\Pi\rangle}[\text{desc}(\mathcal{B}\text{order}_{\Pi}^{\delta',\xi,i})] \le \sqrt{\xi}$ for every $i \in [m]$. Plugging it into Equation (81) yields that $\text{border}_{\Pi}(\delta',\xi) = \Pr_{\langle\Pi\rangle}[\text{desc}(\mathcal{B}\text{order}_{\Pi}^{\delta',\xi})] \le m\cdot\sqrt{\xi}$, completing the proof of Lemma 4.26.

Proof of Claim 4.29. Assume toward a contradiction that there exists $i \in [m]$ such that $|\mathcal{N}(i)| \ge 1/\sqrt{\xi}$. Let P_i be the distribution over $\{0,1\}^i$, described by outputting ℓ_i, for $\ell \leftarrow \langle\Pi\rangle$. We get that $\Pr_{\langle\Pi\rangle}[\operatorname{desc}(\mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j),\xi,i})] = P_i(\mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j),\xi,i})$. Since $\mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j),\xi,i} \cap \mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j'),\xi,i} = \emptyset$ for every $j \neq j' \in \mathcal{J}$, it holds that

$$\begin{aligned} 1 &\geq \sum_{j\in\mathcal{J}} P_i\left(\mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j),\xi,i}\right) \\ &\geq \sum_{j\in\mathcal{N}(i)} P_i\left(\mathcal{B}\mathrm{order}_{\Pi}^{\delta'(j),\xi,i}\right) \\ &> |\mathcal{N}(i)| \cdot \sqrt{\xi} \geq 1, \end{aligned}$$

and a contradiction is derived, where the last inequality follows the assumption that $|\mathcal{N}(i)| \geq 1/\sqrt{\xi}$. □

4.3 The Pruning-in-the-Head Attacker

In Section 4.2, the recursive approximated biased-continuation attacker was shown to successfully bias the approximately pruned variant of any protocol. We now use this result to design an attacker that biases *any* protocol. The new attacker applies the approximated biased-continuation attacker as if the attacked protocol is (approximately) pruned, until it reaches a low- or high-value node, and then it switches its behavior to act honestly (i.e., as the protocol prescribes). Named after its strategy, we name it the *pruning-in-the-head attacker.*

To make the discussion simpler, we start with describing the ideal (inefficient) variant of the pruning-in-the-head attacker. Consider the ideal pruned variant of a protocol pruned at some threshold δ, denoted by $\Pi^{[\delta]} = (\mathsf{A}^{[\delta]}, \mathsf{B}^{[\delta]})$ (see Definition 4.18). Being a coin-flipping protocol, the results of Section 3 apply to $\Pi^{[\delta]}$. Specifically, Theorem 3.3 yields that $(\mathsf{A}^{[\delta]})^{(k)}$ successfully biases $\Pi^{[\delta]}$ (as usual, for concreteness, we focus on the attacker for A). For parameters δ and k, the *ideal pruning-in-the-head attacker*, denoted $\mathsf{A}^{(k,\delta)}$, acts as follows: until reaching a pruned node according to δ (i.e., a node whose value is lower than δ or higher than $1-\delta$), it acts like $(\mathsf{A}^{[\delta]})^{(k)}$; when reaching a pruned node, and in the rest of the execution, it acts like the honest party A. Namely, $\mathsf{A}^{(k,\delta)}$ acts as if it is actually attacking the pruned variant of the protocol, instead of the original protocol.

We argue that $\mathsf{A}^{(k,\delta)}$ biases the original protocol almost as well as $(\mathsf{A}^{[\delta]})^{(k)}$ biases the ideal pruned protocol. Consider the protocols $((\mathsf{A}^{[\delta]})^{(k)}, \mathsf{B}^{[\delta]})$ and $(\mathsf{A}^{(k,\delta)}, \mathsf{B})$. On unpruned nodes, both protocols act the same. On low-value nodes, the protocols might have different control schemes, but their outputs share the same distribution. On high-value nodes, the value of $((\mathsf{A}^{[\delta]})^{(k)}, \mathsf{B}^{[\delta]})$ might be as high as 1, since $(\mathsf{A}^{[\delta]})^{(k)}$ attacks such nodes. On the other hand, in $(\mathsf{A}^{(k,\delta)}, \mathsf{B})$, when a high-value node is reached, $\mathsf{A}^{(k,\delta)}$ acts honestly. However, since this is a high-value node, its value is at least $1-\delta$. All in all, the values of the two protocols differ by at most δ. Hence, $\mathsf{A}^{(k,\delta)}$ successfully attacks (the nonpruned) protocol Π. This might not seem like a great achievement. An inefficient, and much simpler, attack on protocol Π was already presented in Section 3. The point is that unlike the attack of Section 3, the above attacker can be made efficient.

In the rest of this section, we extend the above discussion for approximated attackers attacking approximately pruned protocols. Specifically, we give an approximated variant of $\mathsf{A}^{(k,\delta)}$—the pruning-in-the-head attacker—and prove that it is a successful attacker by showing that it biases *any* protocol Π almost as well as the recursive approximated biased-continuation attacker biases the δ-approximately pruned variant of Π (the latter, by Section 4.2, is a successful attack). In Section 4.4, we show how to implement this attacker using only an honest continuator for the original protocol, which is the main step toward implementing it efficiently assuming the inexistence of one-way functions (done in Section 4.5).

The pruning-in-the-head attacker. Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol. Recall that $\mathsf{HonCont}_{\Pi}^{\xi}$ stands for the arbitrarily fixed ξ-honest continuator for Π (see Definition 4.19) and that Est_{Π}^{ξ} stands for the arbitrarily fixed ξ-estimator for Π (see Definition 4.20). Furthermore, recall that $\mathcal{S}\mathsf{mall}_{\Pi}^{\delta, \mathsf{Est}_{\Pi}^{\xi}}$ ($\mathcal{L}\mathsf{arge}_{\Pi}^{\delta, \mathsf{Est}_{\Pi}^{\xi}}$, respectively) stands for the set of nodes for which Est_{Π}^{ξ} is at most δ (at least $1 - \delta$, respectively) (see Definition 4.21) and that $\Pi^{[\delta, \xi]}$ stands for the (δ, ξ)-approximately pruned variant of Π (see Definition 4.22). Finally, recall that for a set of nodes $\mathcal{S} \subseteq \mathcal{V}(\Pi)$, $\operatorname{desc}(\mathcal{S})$ stands for those nodes that at least one of their predecessors belong to $\mathcal{S}$ (see Definition 2.1).

Let $\widehat{\mathsf{A}}_{\Pi}^{(i, \xi, \delta)} \equiv \mathsf{A}$ and for integer $i > 0$ define:

Algorithm 4.30 (The Pruning-in-the-Head Attacker $\widehat{\mathsf{A}}_{\Pi}^{(i, \xi, \delta)}$).

```
Parameters: integer $i > 0$, $\xi, \delta \in (0, 1)$.
Input: transcript $u \in \{0, 1\}^*$.
Notation: let $\widetilde{\Pi} = \Pi^{[2\delta, \xi]}$.
Operation:
  (1) If $u \in \mathcal{L}(\Pi)$, output $\chi_{\Pi}(u)$ and halt.
  (2) Set msg as follows.
      • If $u \in \operatorname{desc}(\mathcal{S}\mathsf{mall}_{\Pi}^{2\delta, \mathsf{Est}_{\Pi}^{\xi}} \cup \mathcal{L}\mathsf{arge}_{\Pi}^{2\delta, \mathsf{Est}_{\Pi}^{\xi}})$, set $\mathsf{msg} = \mathsf{HonCont}_{\Pi}^{\xi}(u)$.
      • Otherwise, set $\mathsf{msg} = \mathsf{A}_{\widetilde{\Pi}}^{(i, \xi, \delta)}(u)$ (see Algorithm 4.3).
  (3) Send msg to B.
  (4) If $u' = u \circ \mathsf{msg} \in \mathcal{L}(\Pi)$, output $\chi_{\Pi}(u')$.
```

The next lemma lower-bounds the success probability of the pruning-in-the-head attacker. It states that if a given protocol Π does not have many nodes whose value is close to 2δ, then the pruning-in-the-head attacker biases Π almost as well as the approximated attacker biases the approximated pruned protocol.

Recall that $\mathsf{border}_{\Pi}(\delta, \xi)$ stands for the probability that Π generates transcripts whose values are ξ-close to δ or to $1 - \delta$ (see Definition 4.23).

Lemma 4.31 (Main Lemma for the Pruning-in-the-Head Attacker). *Let $0 < \delta \leq \delta' \leq \frac{1}{4}$, let $\xi \in (0, 1)$, and let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[2\delta', \xi]}$ be the $(2\delta', \xi)$-approximately pruned variant of an m-round protocol $\Pi = (\mathsf{A}, \mathsf{B})$ (see Definition 4.22). Then*

$$\begin{aligned}\mathsf{val}\left(\widehat{\mathsf{A}}_{\Pi}^{(k, \xi, \delta')}, \mathsf{B}\right) \geq \mathsf{val}\left(\mathsf{A}_{\widetilde{\Pi}}^{(k)}, \widetilde{\mathsf{B}}\right) &- 2\delta' - (m + 2) \cdot \sqrt{\xi} \\ &- 2 \cdot \phi_{k,\delta}^{\mathsf{Bal}}\left(\mathsf{border}_{\Pi}(2\delta', \xi) + 12 \cdot m \cdot \xi / \delta', 2\sqrt{\xi}, 2 \cdot m \cdot \xi, m, \delta', \mu\right) \\ &- 3 \cdot \phi_{k,\delta}^{\mathsf{It}}(\mathsf{border}_{\Pi}(2\delta', \xi) + 12 \cdot m \cdot \xi / \delta', \xi, m, \delta', \mu),\end{aligned}$$

for every $k \in \mathbb{N}$ and $\mu \in (0, 1)$, and for $\phi_{k,\delta}^{\mathsf{It}}, \phi_{k,\delta}^{\mathsf{Bal}} \in \mathsf{poly}$ according to Lemmas 4.4 and 4.5, respectively.

The rest of this section is dedicated to proving Lemma 4.31.

4.3.1 *Proving Lemma 4.31.*

The proof follows the proof we sketched above for the ideal pruning-in-the-head attacker. When moving to the approximated case, however, we need to consider *failing transcripts*—transcripts on which the approximating oracles fail to give a good approximation. As long as the approximated pruning-in-the-head attacker did not generate a failing transcript, it will succeed in biasing the protocol almost as well as its ideal variant. Thus, the heart of the proof is showing that the approximated pruning-in-the-head attacker generates a failing transcript with only low probability. By definition, the probability of the original protocol to generate such failing transcripts is low, so we can use Lemma 4.25 to argue that the recursive approximated biased-continuation attacker, when attacking the *approximated pruned protocol*, also generates failing transcripts with only low probability. We use this fact to argue that the approximated pruning-in-the-head attacker attacks such transcripts with only low probability as well.

The proof handles separately the failing transcripts into transcripts that *precede* pruned transcripts, i.e., the execution of the protocol has not pruned before generating these transcripts, and the rest of the failing transcripts (i.e., failing transcripts *preceded by* pruned transcripts). Specifically, we make the following observations:

(1) Failing transcripts that precede pruned transcripts (high- or low-value transcripts).
The probability of the approximated pruning-in-the-head attacker to reach these transcripts is the same as the recursive approximated biased-continuation attacker, which we already know is low.
(2) Failing transcript preceded by pruned transcripts. We consider the following two subcases:
   (a) The probability of the original protocol to generate pruned transcripts is low.
   In this case, it suffices to show that the approximated pruning-in-the-head attacker generates pruned transcripts with low probability as well. By Lemma 4.25, the probability of the recursive approximated biased-continuation attacker to generate pruned transcripts is low, and until reaching such transcripts, the approximated pruning-in-the-head attacker acts as the recursive approximated biased-continuation attacker.
   (b) The probability of the original protocol to generate pruned transcripts is high.
   In this case, since, by definition, the overall probability of generating failing transcripts is low, the probability of the original protocol to generate failing transcripts *given that the protocol reached a pruned transcript* is low. Once it reaches a pruned transcript, the pruning-in-the-head attacker behaves just like the original protocol. Thus, the probability that the pruning-in-the-head attacker generates failing transcripts, even conditioning that it generates pruned transcripts, is low.

All in all, we get that the probability that the approximated pruning-in-the-head attacker generates failing transcripts is low, and thus the intuition from the ideal case applies.

Moving to the formal proof, fix $k > 0$ (the proof for $k = 0$ is immediate) and $\mu \in (0, 1)$. To ease notation ahead, let $\gamma_\Pi(\delta', \xi) = \mathsf{border}_\Pi(2\delta', \xi) + 12 \cdot m \cdot \xi / \delta'$. We define four hybrid protocols to establish the above arguments step by step. The proof of the lemma will follow by showing that these hybrid protocols' expected outcomes are close to one another.

Let $\mathcal{F}\mathsf{ail}\mathcal{C}\mathsf{ont} := \{u \in \mathcal{V}(\Pi) : \mathsf{SD}(\mathsf{HonCont}_\Pi^\xi(u), \mathsf{HonCont}(u)) > \xi\}$, i.e., transcripts on which the approximated honest continuator $\mathsf{HonCont}_\Pi^\xi$ acts significantly different from the ideal honest continuator $\mathsf{HonCont}$. Let $\mathcal{F}\mathsf{ail}\mathcal{E}\mathsf{st}$ be the set of low-value transcripts that the approximated estimator Est_Π^ξ mistakenly estimates their value to be high; that is, $\mathcal{F}\mathsf{ail}\mathcal{E}\mathsf{st} := \{u \in \mathcal{V}(\Pi) : \mathsf{val}(\Pi_u) < 1 - 2\delta' - \xi \wedge \mathsf{Est}_\Pi^\xi(u) > 1 - 2\delta'\}$. Let $\mathcal{F}\mathsf{ail} := \mathcal{F}\mathsf{ail}\mathcal{C}\mathsf{ont} \cup \mathcal{F}\mathsf{ail}\mathcal{E}\mathsf{st}$. Finally, let $\mathcal{S}\mathsf{afe}\mathcal{L}\mathsf{arge} := \mathcal{L}\mathsf{arge}_\Pi^{2\delta', \xi} \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail})$, i.e., high-value transcripts that are not descendants of failing transcripts.

We are now ready to define the hybrid protocols, all of which share the common output function of the original protocol Π (i.e., the function determines the common output of full transcripts of Π, see Definition 2.6).

- **Protocol Π_1:** This protocol is just protocol $(\mathsf{A}^{(k,\delta',\xi)}_{\widetilde{\Pi}}, \widetilde{\mathsf{B}})$; i.e., the approximated recursive biased-continuation attacker attacks the approximated pruned protocol.
- **Protocol Π_2:** Both parties act as in Π_1 until (if at all) the first time the protocol's transcript is in $\mathcal{S}\text{afe}\mathcal{L}\text{arge}$. In the rest of the protocol, the parties act like in Π (which also means following Π's control scheme).
- **Protocol Π_3:** Both parties act as in Π_2 until (if at all) the first time the protocol's transcript is in $\mathcal{F}\text{ail}$. In the rest of the protocol, the parties act like in $(\widehat{\mathsf{A}}^{(k,\xi,\delta')}_{\Pi}, \mathsf{B})$ (which also means following $(\widehat{\mathsf{A}}^{(k,\xi,\delta')}_{\Pi}, \mathsf{B})$'s control scheme, which is identical to Π's).
- **Protocol Π_4:** This protocol is just protocol $(\widehat{\mathsf{A}}^{(k,\xi,\delta')}_{\Pi}, \mathsf{B})$, i.e., the approximated pruning-in-the-head attacker attacks the original protocol Π. (This is the protocol whose value we are trying to analyze.)

The proof of the lemma immediately follows the next sequence of claims.

Claim 4.32. *It holds that* $\mathsf{val}(\Pi_2) \geq \mathsf{val}(\Pi_1) - 2\delta' - \xi$.

Proof. Note that protocols Π_1 and Π_2 are identical until the first time the protocol's transcript is in $\mathcal{S}\text{afe}\mathcal{L}\text{arge}$. Hence, we can couple random executions of protocols Π_1 and Π_2 so that they are the same until the first time the protocol's transcript is in $\mathcal{S}\text{afe}\mathcal{L}\text{arge}$. Hence, for proving that claim, it suffices to show that $\mathsf{val}((\Pi_1)_u) - \mathsf{val}((\Pi_2)_u) \leq 2\delta' + \xi$, for every $u \in \mathsf{frnt}(\mathcal{S}\text{afe}\mathcal{L}\text{arge})$.

Fix $u \in \mathsf{frnt}(\mathcal{S}\text{afe}\mathcal{L}\text{arge})$. Since $u \in \mathcal{L}\text{arge}^{2\delta',\xi}_{\Pi}$, it holds that $\mathsf{Est}^{\xi}_{\Pi}(u) \geq 1 - 2\delta'$. Since $u \notin \mathcal{F}\text{ail}\mathcal{E}\text{st}$, it holds that $\mathsf{val}(\Pi_u) \geq 1 - 2\delta' - \xi$. Once visiting u, the parties in Π_2 act like in Π. Thus, it holds that $\mathsf{val}((\Pi_2)_u) = \mathsf{val}(\Pi_u)$. Since it is always the case that $\mathsf{val}((\Pi_1)_u) \leq 1$, we have $\mathsf{val}((\Pi_1)_u) - \mathsf{val}((\Pi_2)_u) \leq 2\delta' + \xi$. □

Claim 4.33. *It holds that*

$$\mathsf{val}(\Pi_3) \geq \mathsf{val}(\Pi_2) - \sqrt{\xi} - 2 \cdot \phi^{\mathsf{Bal}}_{k,\delta}\left(\gamma_\Pi(\delta',\xi), 2\sqrt{\xi}, 2 \cdot m \cdot \xi, m, \delta', \mu\right)$$
$$- 2 \cdot \phi^{\mathsf{It}}_{k,\delta}(\gamma_\Pi(\delta',\xi), \xi, m, \delta', \mu).$$

Proof. We prove the claim by proving the following, stronger statement:

$$\mathsf{SD}(\langle \Pi_2 \rangle, \langle \Pi_3 \rangle) \leq \sqrt{\xi} + 2 \cdot \phi^{\mathsf{Bal}}_{k,\delta}\left(\gamma_\Pi(\delta',\xi), 2\sqrt{\xi}, 2 \cdot m \cdot \xi, m, \delta', \mu\right)$$
$$+ 2 \cdot \phi^{\mathsf{It}}_{k,\delta}(\gamma_\Pi(\delta',\xi), \xi, m, \delta', \mu).$$

Note that protocols Π_2 and Π_3 are identical until the first time the protocol's transcript is in $\mathcal{F}\text{ail}$. Hence, we can couple random executions of protocols Π_2 and Π_3 so that the executions are the same until the first time the protocol's transcript is in $\mathcal{F}\text{ail}$. Thus, it suffices to show that

$$\Pr_{\langle \Pi_2 \rangle}[\mathsf{desc}(\mathcal{F}\text{ail})] \leq \sqrt{\xi} + 2 \cdot \phi^{\mathsf{Bal}}_{k,\delta}\left(\gamma_\Pi(\delta',\xi), 2\sqrt{\xi}, 2 \cdot m \cdot \xi, m, \delta', \mu\right) \tag{82}$$
$$+ 2 \cdot \phi^{\mathsf{It}}_{k,\delta}(\gamma_\Pi(\delta',\xi), \xi, m, \delta', \mu).$$

Let $\mathcal{F}_1 = \mathcal{F}\text{ail} \cap \mathsf{desc}(\mathcal{S}\text{afe}\mathcal{L}\text{arge})$ and $\mathcal{F}_2 = \mathcal{F}\text{ail} \setminus \mathcal{F}_1$. Since

$$\Pr_{\langle \Pi_2 \rangle}[\mathsf{desc}(\mathcal{F}\text{ail})] \leq \Pr_{\langle \Pi_2 \rangle}[\mathsf{desc}(\mathcal{F}_1)] + \Pr_{\langle \Pi_2 \rangle}[\mathsf{desc}(\mathcal{F}_2)], \tag{83}$$

it suffices to bound the two summands in the right-hand side of Equation (83). We begin by bounding the second summand. Since $\mathcal{F}_2 \subseteq \mathcal{F}\text{ail}$, and by the definitions of $\mathsf{HonCont}^{\xi}_{\Pi}$ and Est^{ξ}_{Π}, it holds that

$$\Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}_2)] \leq \Pr_{\langle \Pi \rangle}[\mathsf{desc}(\mathcal{F}\text{ail})] \leq 2\xi. \tag{84}$$

As we did in the proof of the previous claim, we couple random executions of protocols Π_1 and Π_2 so that the executions are the same until the first time the protocol's transcript is in $\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}$. Since transcripts in $\mathcal{F}_2$ are not descendants of $\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}$, it holds that

$$\begin{aligned}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(\mathcal{F}_2)] &= \Pr_{\langle\Pi_1\rangle}[\mathrm{desc}(\mathcal{F}_2)] \\ &= \Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(k,\xi,\delta')},\widetilde{\mathsf{B}}\right\rangle}[\mathrm{desc}(\mathcal{F}_2)] \\ &\le \phi_{k,\delta}^{\mathsf{Bal}}(\gamma_\Pi(\delta',\xi),2\xi,2\cdot m\cdot\xi,m,\delta',\mu)+\phi_{k,\delta}^{\mathsf{It}}(\gamma_\Pi(\delta',\xi),\xi,m,\delta',\mu),\end{aligned} \tag{85}$$

where the second equality follows from the definition of Π_1, and the inequality follows from Lemma 4.25.

We now bound the first summand in the right-hand side of Equation (83). Let

$$\mathcal{S}_1 = \left\{u\in \mathsf{frnt}(\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}) : \Pr_{\langle\Pi_u\rangle}[\mathrm{desc}(\mathcal{F}_1)] \ge \sqrt{\xi}\right\}$$

and

$$\mathcal{S}_2 = \left\{u\in \mathsf{frnt}(\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}) : 0 < \Pr_{\langle\Pi_u\rangle}[\mathrm{desc}(\mathcal{F}_1)] < \sqrt{\xi}\right\}.$$

Namely, $\mathcal{S}_1$ are those nodes (transcripts) in the frontier of $\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}$ from which there is high probability (larger than $\sqrt{\xi}$) that Π reaches $\mathcal{F}_1$. On the other hand, $\mathcal{S}_2$ are those nodes in the frontier of $\mathcal{S}\mathrm{afe}\mathcal{L}\mathrm{arge}$ from which there is low probability (positive, but less than $\sqrt{\xi}$) that Π reaches $\mathcal{F}_1$. Using the above coupling between Π_1 and Π_2, it follows that

$$\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(\mathcal{F}_1)] \le \Pr_{\langle\Pi_1\rangle}[\mathrm{desc}(\mathcal{S}_1)] + \Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(\mathcal{F}_1\cap\mathrm{desc}(\mathcal{S}_2))]. \tag{86}$$

Again, we bound each term in the right-hand side of the above equation separately. For the first term of Equation (86), it holds that

$$2\xi \ge \Pr_{\langle\Pi\rangle}[\mathrm{desc}(\mathcal{F}\mathrm{ail})] \ge \Pr_{\langle\Pi\rangle}[\mathrm{desc}(\mathcal{F}_1)] \ge \Pr_{\langle\Pi\rangle}[\mathrm{desc}(\mathcal{S}_1)]\cdot\sqrt{\xi},$$

and thus $\Pr_{\langle\Pi\rangle}[\mathrm{desc}(\mathcal{S}_1)] \le 2\sqrt{\xi}$. Applying Lemma 4.25 again yields that

$$\begin{aligned}\Pr_{\langle\Pi_1\rangle}[\mathrm{desc}(\mathcal{S}_1)] &\le \Pr_{\left\langle \mathsf{A}_{\widetilde{\Pi}}^{(k,\xi,\delta')},\widetilde{\mathsf{B}}\right\rangle}[\mathrm{desc}(\mathcal{S}_2)] \\ &\le \phi_{k,\delta}^{\mathsf{Bal}}\left(\gamma_\Pi(\delta',\xi),2\sqrt{\xi},2\cdot m\cdot\xi,m,\delta',\mu\right)+\phi_{k,\delta}^{\mathsf{It}}(\gamma_\Pi(\delta',\xi),\xi,m,\delta',\mu).\end{aligned} \tag{87}$$

As for the second term of Equation (86), we write

$$\begin{aligned}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(\mathcal{F}_1\cap\mathrm{desc}(\mathcal{S}_2))] &= \sum_{u\in\mathcal{S}_2}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(u)]\cdot\Pr_{\langle(\Pi_2)_u\rangle}[\mathrm{desc}(\mathcal{F}_2)] \\ &= \sum_{u\in\mathcal{S}_2}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(u)]\cdot\Pr_{\langle\Pi_u\rangle}[\mathrm{desc}(\mathcal{F}_2)] \\ &\le \sqrt{\xi}\cdot\sum_{u\in\mathcal{S}_2}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(u)] \\ &\le \sqrt{\xi},\end{aligned} \tag{88}$$

where the second inequality follows from the definition of Π_2.

Plugging Equations (87) and (88) into Equation (86) yields that

$$\begin{aligned}\Pr_{\langle\Pi_2\rangle}[\mathrm{desc}(\mathcal{F}_1)] \le \sqrt{\xi} &+ \phi_{k,\delta}^{\mathsf{Bal}}\left(\gamma_\Pi(\delta',\xi),2\sqrt{\xi},2\cdot m\cdot\xi,m,\delta',\mu\right) \\ &+ \phi_{k,\delta}^{\mathsf{It}}(\gamma_\Pi(\delta',\xi),\xi,m,\delta',\mu).\end{aligned} \tag{89}$$

Equation (82) follows by plugging Equations (85) and (89) into Equation (83) and noting that replacing ξ by $\sqrt{\xi}$ in the second variable of the function $\phi_{k,\delta}^{\mathsf{Bal}}$ only increases it. □

Claim 4.34. *It holds that* $\mathsf{val}(\Pi_4) \geq \mathsf{val}(\Pi_3) - m \cdot \xi$.

Proof. We prove the claim by proving the following, stronger, statement:

$$\mathsf{SD}(\langle \Pi_3 \rangle, \langle \Pi_4 \rangle) \leq m \cdot \xi. \tag{90}$$

Let $\mathcal{L}\mathsf{arge} = \mathcal{L}\mathsf{arge}_{\Pi}^{2\delta, \mathsf{Est}_{\Pi}^{\xi}}$ and $\mathcal{S}\mathsf{mall} = \mathcal{S}\mathsf{mall}_{\Pi}^{2\delta, \mathsf{Est}_{\Pi}^{\xi}}$. We start by defining two randomized functions $f, g : \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi) \to \mathcal{V}(\Pi)$, to simulate Π_3 and Π_4, respectively. Let

$$f(u) = \begin{cases} \ell_{1,\ldots,|u|+1} \text{ for } \ell \leftarrow \left(\mathsf{A}_{\widetilde{\Pi}}^{(k,\delta',\xi)}, \widetilde{\mathsf{B}}\right)_u & u \notin \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge} \cup \mathcal{S}\mathsf{mall}) \\ \mathsf{HonCont}(u)_{1,\ldots,|u|+1} & u \in \mathsf{desc}(\mathcal{L}\mathsf{arge}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail}) \\ \mathsf{HonCont}^{\xi}(u)_{1,\ldots,|u|+1} & u \in \mathsf{desc}(\mathcal{S}\mathsf{mall}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge}) \\ \ell_{1,\ldots,|u|+1} \text{ for } \ell \leftarrow \left(\widehat{\mathsf{A}}_{\Pi}^{(k,\xi,\delta')}, \mathsf{B}\right)_u & u \in \mathsf{desc}(\mathcal{F}\mathsf{ail}), \end{cases}$$

and let

$$g(u) = \begin{cases} f(u) & u \notin \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge} \cup \mathcal{S}\mathsf{mall}) \\ \mathsf{HonCont}^{\xi}(u)_{1,\ldots,|u|+1} & u \in \mathsf{desc}(\mathcal{L}\mathsf{arge}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{A}} \\ f(u) & u \in \mathsf{desc}(\mathcal{L}\mathsf{arge}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{B}} \\ f(u) & u \in \mathsf{desc}(\mathcal{S}\mathsf{mall}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{A}} \\ \mathsf{HonCont}(u)_{1,\ldots,|u|+1} & u \in \mathsf{desc}(\mathcal{S}\mathsf{mall}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{B}} \\ f(u) & u \in \mathsf{desc}(\mathcal{F}\mathsf{ail}). \end{cases}.$$

Namely, for $u \in \mathsf{desc}(\mathcal{L}\mathsf{arge}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{A}}$, $f(u) = \mathsf{HonCont}(u)_{1,\ldots,|u|+1}$, while $g(u) = \mathsf{HonCont}^{\xi}(u)_{1,\ldots,|u|+1}$, where for $u \in \mathsf{desc}(\mathcal{S}\mathsf{mall}) \setminus \mathsf{desc}(\mathcal{F}\mathsf{ail} \cup \mathcal{L}\mathsf{arge}) \cap \mathcal{C}\mathsf{trl}_{\Pi}^{\mathsf{B}}$, $f(u) = \mathsf{HonCont}^{\xi}(u)_{1,\ldots,|u|+1}$, while $g(u) = \mathsf{HonCont}(u)_{1,\ldots,|u|+1}$. For any other u, $f(u) = g(u)$.

Let H^h be the process that repeatedly calls the function h with the answer of the previous call, starting with $h(\mathsf{root}(\Pi))$, until reaching a leaf. It is easy to verify that $\mathsf{H}^f \equiv \langle \Pi_3 \rangle$ and $\mathsf{H}^g \equiv \langle \Pi_4 \rangle$. Thus, is suffices to bound $\mathsf{SD}(\mathsf{H}^f, \mathsf{H}^g)$. By the definitions of f and g, it holds that $\mathsf{SD}(f(u), g(u)) = 0$ if $u \in \mathcal{F}\mathsf{ail}$ and that $\mathsf{SD}(f(u), g(u)) \leq \mathsf{SD}(\mathsf{HonCont}^{\xi}(u), \mathsf{HonCont}(u)) \leq \xi$ if $u \notin \mathcal{F}\mathsf{ail}$, where the last inequality follows from the definition of $\mathcal{F}\mathsf{ail}$. The claim follows since H^h makes at most m calls to h. □

Using the above claims, we can formally prove Lemma 4.31.

Proof of Lemma 4.31. Fix $k \in \mathbb{N}$ and $\mu \in (0, 1)$. Claims 4.32 to 4.34 yield that

$$\begin{aligned} \mathsf{val}\left(\widehat{\mathsf{A}}_{\Pi}^{(k,\xi,\delta')}, \mathsf{B}\right) \geq{}& \mathsf{val}\left(\mathsf{A}_{\widetilde{\Pi}}^{(k,\delta',\xi)}, \widetilde{\mathsf{B}}\right) - 2\delta' - (m+2) \cdot \sqrt{\xi} \\ & - 2 \cdot \phi_{k,\delta}^{\mathsf{Bal}}\left(\gamma_{\Pi}(\delta', \xi), 2\sqrt{\xi}, 2 \cdot m \cdot \xi, m, \delta', \mu\right) \\ & - 2 \cdot \phi_{k,\delta}^{\mathsf{It}}(\gamma_{\Pi}(\delta', \xi), \xi, m, \delta', \mu). \end{aligned}$$

The proof now follows from Lemma 4.24. □

4.4 Implementing the Pruning-in-the-Head Attacker Using an Honest Continuator

The pruning-in-the-head attacker (Algorithm 4.30) uses the honest continuator and the estimator algorithms (see Definitions 4.19 and 4.20, respectively), both defined with respect to the attacked (original) protocol. It also uses the recursive approximated biased-continuation attacker (see Algorithm 4.3), designed to attack the approximately pruned variant of the attacked protocol. In this section, we show how to use a given honest continuator for implementing the other two algorithms the pruning-in-the-head attacker uses. It follows that implementing the pruning-in-the-head attacker reduces to implementing an honest continuator. In the next (and final) section, we show how to implement such a continuator assuming the inexistence of one-way functions.

We begin by showing that using an honest continuator and an estimator, one can implement a biased continuator for the approximated pruned protocol. In fact, due to the recursive nature of the attack, we need to implement a biased continuator for every level of the recursion, and not only for the approximated pruned protocol.

Definition 4.35. Let $\Pi = (\mathsf{A}, \mathsf{B})$ be a protocol, let $\delta, \xi \in (0,1)$, let $k \in \mathbb{N}$, and let $\{\mathsf{D}^{(i)}\}_{i \in (k)}$ be a set of algorithms. Let $\Pi^{(0)} = \Pi$. For $i \in [k]$, let $\Pi^{(i)} = (\mathsf{A}^{(i,\xi,\delta)}_{\mathsf{D}^{(i-1)}}, \mathsf{B})$, where $\mathsf{A}^{(i,\xi,\delta)}_{\mathsf{D}^{(i-1)}}$ acts as $\mathsf{A}^{(i,\xi,\delta)}_{\Pi}$ (Algorithm 4.3) does, but with $\mathsf{D}^{(i-1)}$ taking the role of $\mathsf{BiasedCont}^{\xi,\delta}_{(\mathsf{A}^{(i-1,\xi,\delta)}_{\Pi},\mathsf{B})}$.[54] The sequence $\{\mathsf{D}^{(i)}\}_{i \in (k)}$ is a (ξ, δ)-biased-continuators sequence for Π, if algorithm $\mathsf{D}^{(i)}$ is a (ξ,δ)-biased continuator of $\Pi^{(i)}$, for every $i \in (k)$.

Lemma 4.36. *Let Π be an m-round protocol. Let $\delta \in (0, 1/2)$, let $\xi \in (0,1)$, let Est be a $[0,1]$-output deterministic algorithm, let HC be a ξ-honest-continuator for Π, and let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[2\delta,\xi,\mathsf{Est},\mathsf{HC}]}$ be the $(\delta, \mathsf{Est}, \mathsf{HC})$-approximately pruned variant of Π (see Definition 4.22). Then, for every $k \in \mathbb{N}$, there exists a sequence of algorithms $\{\mathsf{D}^{(i)}\}_{i \in (k)}$ with the following properties:*

(1) *$\{\mathsf{D}^{(i)}\}_{i \in (k)}$ is a (ξ, δ)-biased-continuators sequence for $\widetilde{\Pi}$.*
(2) *$\mathsf{D}^{(k)}$'s running time is $O(m^{3(k+1)} \cdot \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil^{k+1} \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}}))$, with T_{Est} and T_{HC} being the running times of Est and HC, respectively.*

Lemma 4.36 is proven in Section 4.4.1. Next, we show how to implement a *randomized* estimator using an honest continuator.

Lemma 4.37. *Let Π be an m-round protocol, let $\xi \in (0,1)$, and let HC be a $\xi/2$-honest continuator for Π. Then there exists a randomized algorithm $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi}$ such that the following holds:*

(1) *$\Pr_{r \leftarrow \{0,1\}^\ell}[\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi,r}$ is a ξ-*estimator for Π*$] \geq 1 - \xi$, with ℓ being an upper bound on the number coins used by $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi}$ including those used by HC, and $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi,r}$ being the deterministic algorithm defined by hard-wiring r into the randomness of $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi}$.*
(2) *$\mathsf{Est}^{(\xi,\mathsf{HC})}$'s running time is $O(m \cdot \lceil \frac{\ln(2^m/\xi)}{\xi^2/2} \rceil \cdot T_{\mathsf{HC}})$, with T_{HC} being the running time of HC.*

Lemma 4.37 is proven in Section 4.4.2. Using the above implementations for a biased continuator and an estimator, we can define an implantation for the pruning-in-the-head attacker using only an honest continuator. Recall that the pruning-in-the-head attacker requires a *deterministic* estimator. To get such an estimator, we randomly fix the coins of $\mathsf{Est}^{(\xi,\mathsf{HC})}$.

Definition 4.38 (Algorithm $\widetilde{\mathsf{A}}^{(k,\xi,\delta,\mathsf{HC})}_{\Pi}$). Let $\delta \in (0, 1/2)$, let $\xi \in (0,1)$, and let $k > 0$. Let Π be an m-round protocol, let HC be an algorithm, and let ℓ be the number of coins used by algorithm $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi}$ from Lemma 4.37, including those used by algorithm HC. For $r \in \{0,1\}^\ell$, let $\mathsf{Est}_r = \mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi;r}$ be the deterministic algorithm resulting from fixing $\mathsf{Est}^{(\xi,\mathsf{HC})}_{\Pi;r}$ coins to r.

Let $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}) = \Pi^{[2\delta,\xi,\mathsf{Est}_r,\mathsf{HC}]}$ and $\mathsf{BiasedCont} = \mathsf{BiasedCont}^{(\xi,\delta,\mathsf{HC},k-1)}_{\widetilde{\Pi}}$, where $\{\mathsf{BiasedCont}^{(\xi,\delta,\mathsf{HC},i)}_{\widetilde{\Pi}}\}_{i \in (k-1)}$ is the (ξ, δ)-biased-continuators sequence for $\widetilde{\Pi}$, guaranteed to

[54] Recall that $\mathsf{BiasedCont}^{\xi,\delta}_{\Pi'}$ is an arbitrary fixed (ξ, δ)-biased continuator of Π'.

exist by Lemma 4.36. Algorithm $\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta,\mathsf{HC})}$ acts as algorithm $\widehat{\mathsf{A}}_{\Pi}^{(k,\xi,\delta)}$ (see Algorithm 4.30), but with algorithms HC, Est_r, and BiasedCont taking the role of algorithms $\mathsf{HonCont}_{\Pi}^{\xi}$, Est_{Π}^{ξ}, and $\mathsf{BiasedCont}_{(\mathsf{A}_{\widetilde{\Pi}}^{(k-1,\xi,\delta)},\widetilde{\mathsf{B}})}^{\xi,\delta}$, respectively. Finally, algorithm $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta,\mathsf{HC})}$ act as $\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta,\mathsf{HC})}$, for $r \leftarrow \{0,1\}^{\ell}$.

The analysis of algorithm $\widehat{\mathsf{A}}_{\Pi}^{(k,\xi,\delta)}$ given in previous sections was done with respect to $\mathsf{HonCont}_{\Pi}^{\xi}$, Est_{Π}^{ξ}, and $\mathsf{BiasedCont}_{(\mathsf{A}_{\widetilde{\Pi}}^{(k-1,\xi,\delta)},\widetilde{\mathsf{B}})}^{\xi,\delta}$, the arbitrary but fixed honest continuator, estimator, and biased continuator (see Definitions 4.2, 4.19, and 4.20). Lemma 4.37 show that Est_r is a ξ-estimator with high probability and Lemma 4.36 shows that BiasedCont is a (ξ,δ)-biased continuator. Since the above fixing was arbitrary, the results from previous sections can be applied to Algorithm $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta,\mathsf{HC})}$ as well. We do so in the next lemma, which also analyzes $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta,\mathsf{HC})}$'s running time.

Lemma 4.39. *Let $\Pi = (\mathsf{A},\mathsf{B})$ be an m-round protocol, let $0 < \delta \le \delta' \le \frac{1}{4}$, $\xi \in (0,1)$, $k > 0$, and let* HC *be a $\xi/2$-honest continuator for Π. The following holds with respect to Algorithm $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$:*

(1)

$$\begin{aligned}\mathsf{val}\left(\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})},\mathsf{B}\right) \ge{}& \mathsf{val}\left(\mathsf{A}_{\widetilde{\Pi}}^{(k)},\widetilde{\mathsf{B}}\right) - 2\delta' - (m+2)\cdot\sqrt{\xi} - \xi \\ &- 2\cdot\phi_{k,\delta}^{\mathsf{Bal}}\left(\mathsf{border}_{\Pi}(2\delta',\xi) + 12\cdot m\cdot\xi/\delta', 2\sqrt{\xi}, 2\cdot m\cdot\xi, m, \delta', \mu\right) \\ &- 3\cdot\phi_{k,\delta}^{\mathsf{It}}(\mathsf{border}_{\Pi}(2\delta',\xi) + 12\cdot m\cdot\xi/\delta', \xi, m, \delta', \mu),\end{aligned} \tag{91}$$

for every $\mu \in (0,1)$, and for $\phi_{k,\delta}^{\mathsf{It}}, \phi_{k,\delta}^{\mathsf{Bal}}$ according to Lemmas 4.4 and 4.5, respectively.

(2) $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$'s running time is at most $O(m^{3k+5}\cdot\lceil\frac{\log(1/\xi)}{\log(1/(1-\delta))}\rceil^{k}\cdot\lceil\frac{\ln(2^m/\xi)}{\xi^2/2}\rceil\cdot T_{\mathsf{HC}})$, with T_{HC} being the running time of HC .

Note the extra ξ term in the right-hand side of Equation (91) compared to the term in Lemma 4.31. This term comes from the probability the estimator used by $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$ is not a good one.

Proof. We prove each item separately.

Proof of (1): It holds that

$$\begin{aligned}&\mathsf{val}\left(\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})},\mathsf{B}\right) \\ &\quad\ge \Pr\left[\mathsf{out}\left(\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta',\mathsf{HC})},\mathsf{B}\right) = 1 \;\middle|\; \mathsf{Est}_r \text{ is a } \xi\text{-estimator}\right]\cdot\Pr[\mathsf{Est}_r \text{ is a } \xi\text{-estimator}] \\ &\quad\ge \Pr\left[\mathsf{out}\left(\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta',\mathsf{HC})},\mathsf{B}\right) = 1 \;\middle|\; \mathsf{Est}_r \text{ is a } \xi\text{-estimator}\right] - \xi,\end{aligned} \tag{92}$$

where the second inequality follows from Lemma 4.37. The above probabilities are over the choice of r; the additional, if any, coins of $\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta',\mathsf{HC})}$; and the coins of B.

We would like to conclude the proof by applying Lemma 4.31 to Equation (92). Lemma 4.31 is stated for $\mathsf{HonCont}_{\Pi}^{\xi}$ and Est_{Π}^{ξ}—*arbitrary* ξ-honest-continuator and ξ-estimator for the attacked (original) protocol—and for $\mathsf{BiasedCont}_{(\mathsf{A}_{\widetilde{\Pi}}^{(k-1,\xi,\delta)},\widetilde{\mathsf{B}})}^{\xi,\delta}$—an *arbitrary* (ξ,δ)-biased continuator for $(\mathsf{A}_{\widetilde{\Pi}}^{(k-1,\xi,\delta)},\widetilde{\mathsf{B}})$. By assumption and Lemmas 4.36 and 4.37, HC, Est_r, and BiasedCont are such honest continuator, estimator, and biased continuator, respectively. Hence, the proof of this part is followed by Lemma 4.31.

Proof of (2): The proof is an easy implication of Lemmas 4.36 and 4.37. By definition, $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$ makes a single call to Est and then either calls BiasedCont or HC.[55] We focus on the former case, as the running time of BiasedCont is longer than that of HC. By Lemma 4.37, the running time of Est is $O(m \cdot \lceil \frac{\ln(2^m/\xi)}{\xi^2/2} \rceil \cdot T_{\mathsf{HC}})$, and by Lemma 4.36 and since $\delta \leq \delta'$, the running time of BiasedCont is at most $O(m^{3(k+1)} \cdot \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil^{k+1} \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}}))$. For every call to BiasedCont and Est, algorithm $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$ makes at most $O(m)$ steps. Hence, $\widetilde{\mathsf{A}}_{\Pi}^{(k,\xi,\delta',\mathsf{HC})}$'s running time is bounded by

$$\begin{aligned} &O\left(m \cdot m^{3(k+1)} \cdot \left\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \right\rceil^{k+1} \cdot \left(\left(m \cdot \left\lceil \frac{\ln(2^m/\xi)}{\xi^2/2} \right\rceil \cdot T_{\mathsf{HC}} \right) + T_{\mathsf{HC}} \right) \right) \\ &\quad = O\left(m^{3k+5} \cdot \left\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \right\rceil^{k} \cdot \left\lceil \frac{\ln(2^m/\xi)}{\xi^2/2} \right\rceil \cdot T_{\mathsf{HC}} \right). \end{aligned}$$ □

The rest of this section is dedicated to proving Lemmas 4.36 and 4.37.

4.4.1 Implementing the Biased-Continuation Attacker Using Honest Continuator and Estimator—Proving Lemma 4.36. Our goal is to implement a sequence of biased continuators, denoted by $\{\mathsf{D}^{(i)}\}_{i\in(k)}$, for the approximated pruned protocol $\widetilde{\Pi}$, using only honest continuator HC and an estimator Est for the original (i.e., unpruned) protocol. We do so by a recursive construction.

Given $\{\mathsf{D}^{(i)}\}_{i\in(k-1)}$, a sequence of efficient algorithms such that $\mathsf{D}^{(i)}$ is a (ξ,δ)-biased continuator for $\widetilde{\Pi}^{(i)} = (\mathsf{A}_{\mathsf{D}^{(i-1)}}^{(i,\xi,\delta)}, \widetilde{\mathsf{B}})$, we construct $\mathsf{D}^{(k)}$, an efficient (ξ,δ)-biased continuator for $\widetilde{\Pi}^{(k)}$, as follows. The first step is to reduce the task of implementing a biased continuator for $\widetilde{\Pi}^{(k)}$ to that of implementing a honest continuator for $\widetilde{\Pi}^{(k)}$. This is done using the method of rejection sampling. The second step is to reduce the task of implementing an honest continuator for $\widetilde{\Pi}^{(k)}$ to that of efficiently computing $\widetilde{\Pi}^{(k)}$. A key observation to achieve this task is that $\widetilde{\Pi}^{(k)}$ is *stateless*—namely, the parties do not keep state between the different rounds. And constructing an honest continuator for stateless and efficiently computable protocols is a trivial task. Finally, we note that $\widetilde{\Pi}^{(k)}$ is efficient, assuming that $\mathsf{D}^{(k-1)}$, HC, and Est, are. The section follows this outline to formally prove Lemma 4.36.

From honest continuation to biased continuation. Turning an honest continuator into a biased continuator is essentially an easy task; given a transcript u and a bit b toward which the continuator should bias, sample sufficiently many honest continuations for u, and return the first continuation whose common output is b. Indeed, if the transcript's value (i.e., expected outcome) is close enough to b, then with high probability the above process indeed returns a biased continuation.

Algorithm 4.40 ($\mathsf{BiasedCont}_{\Pi}^{(\xi,\delta,\mathsf{HC})}$).

Parameters: $\xi, \delta \in (0,1)$.
Oracle: HC.
Input: $u \in \mathcal{V}(\Pi)$ *and* $b \in \{0,1\}$.
Operation:

[55] As written in Algorithm 4.30, $\widetilde{\mathsf{A}}_{\Pi;r}^{(k,\xi,\delta',\mathsf{HC})}$ might make m calls to Est (checking whether $u \in \operatorname{desc}(\mathcal{F})$ in step 2 of the algorithm). This, however, does not significantly affect the running time and can be easily avoided by having the attacker keep a state. Furthermore, the time it takes to sample coins for Est is bounded by Est's running time.

```
    (1) For $i = 1$ to $\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil$:
        (a) Set $\ell := \text{HC}(u)$.
        (b) If $\chi_\Pi(\ell) = b$, return $\ell_{|u|+1}$.
    (2) Return $\perp$.
```

Claim 4.41. *Let Π be an m-round protocol, let $\xi, \xi', \delta \in (0,1)$, and let* HC *be a ξ'-honest continuator for Π. Then $\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HC})}$ is a $((t+1) \cdot \xi' + \xi, \delta)$-biased continuator for Π, for $t = \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil$.*

Proof. Let HonCont_Π be the algorithm that on input u returns a random element in $\langle \Pi_u \rangle$, and recall the definition of BiasedCont_Π from Definition 3.1. As usual, we focus on proving the statement for algorithms trying to bias toward one, i.e., $b = 1$; the proof for the case that $b = 0$ is analogous. We show that for every node $u \in \mathcal{V}(\Pi)$ with $\text{SD}(\text{HC}(u), \text{HonCont}_\Pi(u)) \leq \xi'$, and $\text{val}(\Pi_u) \geq \delta$, it holds that

$$\text{SD}\left(\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HC})}(u,1), \text{BiasedCont}_\Pi(u,1)\right) \leq t \cdot \xi' + \xi. \tag{93}$$

This suffices to complete the proof since HC is a ξ'-honest continuator for Π, and thus the probability that Π generates a transcript u such that $\text{SD}(\text{HC}(u), \text{HonCont}_\Pi(u)) > \xi'$ is at most ξ'. The following is an "unbounded version" of algorithm $\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HC})}(\cdot, 1)$ defined above. □

Algorithm 4.42 ($\widehat{\text{BiasedCont}}$).

```
  Input: $u \in \mathcal{V}(\Pi)$.
  Operation:
    (1) Do (forever):
        (a) Set $\ell := \text{HonCont}_\Pi(u)$.
        (b) If $\chi_\Pi(\ell) = 1$, return $\ell_{|u|+1}$.
```

It is not difficult to verify that the probability that $\widehat{\text{BiasedCont}}(u)$ does not halt is zero for every u with $\text{val}(\Pi_u) > 0$. Fix u with $\text{SD}(\text{HC}(u), \text{HonCont}_\Pi(u)) \leq \xi'$, and $\text{val}(\Pi_u) \geq \delta$. It holds that

$$\text{BiasedCont}_\Pi(u,1) \equiv \widehat{\text{BiasedCont}}(u). \tag{94}$$

The only difference between $\widehat{\text{BiasedCont}}(u)$ and algorithm $\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HonCont}_\Pi)}(u,1)$ (i.e., HonCont_Π is taking the role of HC in Algorithm 4.40) is the probability the latter output $\perp$. Hence,

$$\text{SD}\left(\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HonCont})}(u,1), \widehat{\text{BiasedCont}}(u)\right) \leq \Pr\left[\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HonCont})}(u,1) = \perp\right]. \tag{95}$$

Compute

$$\begin{aligned} \Pr\left[\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HonCont})}(u,1) = \perp\right] &= \left(\Pr_{\ell \leftarrow \text{HonCont}(u)}[\chi_\Pi(\ell) = 0]\right)^t \\ &\leq (1-\delta)^t \\ &\leq \xi, \end{aligned}$$

where the first inequality follows since $\text{val}(\Pi_u) \geq \delta$ and the last inequality follows from the choice of t. Moreover, since $\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HC})}$ makes t calls to its oracle, the assumption that $\text{SD}(\text{HonCont}(u), \text{HC}(u)) \leq \xi'$ and a standard hybrid argument yield that

$$\text{SD}\left(\text{BiasedCont}_\Pi^{(\xi,\delta,\text{HonCont})}(u,1), \text{BiasedCont}_\Pi^{(\xi,\delta,\text{HC})}(u,1)\right) \leq t \cdot \xi.$$

A triangle inequality now completes the proof of Equation (93), and thus of the claim. □

Honest continuator for stateless protocols. For stateless protocols (i.e., the parties maintain no state), implementing (perfect) honest continuation is trivial.

ALGORITHM 4.43 ($\mathsf{HonContSL}_\Pi$).

```
Input: transcript $u \in \{0,1\}^*$.
Operation:
    (1) Set $t = u$.
    (2) Repeat until $t \in \mathcal{L}(\Pi)$:
        (a) Let $\mathsf{C}$ be the party that controls $t$.
        (b) Sample uniformly at random coins $r_\mathsf{C}$ for this round.
        (3) Set $t = t \circ \mathsf{C}(t; r_\mathsf{C})$.
    (3) Return $t$.
```

CLAIM 4.44. *For a stateless protocol* Π*, algorithm* $\mathsf{HonContSL}_\Pi$ *of Algorithm 4.43 is a 0-honest continuator.*

PROOF. Immediate. □

Proving Lemma 4.36. We now use the above understanding (Claims 4.41 and 4.44) to prove Lemma 4.36.

PROOF OF LEMMA 4.36. The proof is by induction on k. We show that the running time of $\mathsf{D}^{(k)}$ is at most $c^{k+1} \cdot m^{2(k+1)} \cdot \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil^{k+1} \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}})$ for some constant $c > 0$ to be determined by the analysis. The running time as stated in the lemma follows since $c^{k+1} \in O(m^{k+1})$.

For the base case $k = 0$, the (ξ,δ)-biased continuator for $\widetilde{\Pi}$ is defined by

$$\mathsf{D}^{(0)} = \mathsf{BiasedCont}_\Pi^{(\xi,\delta,\mathsf{HonContSL}_{\widetilde{\Pi}})}.$$

Namely, $\mathsf{D}^{(0)}$ is Algorithm 4.40, with Algorithm 4.43 being the honest continuator. Claims 4.41 and 4.44 and the fact that, by definition (recall Definition 4.22), $\widetilde{\Pi}$ is stateless yield that $\mathsf{D}^{(0)}$ is indeed a (ξ,δ)-biased continuator for $\widetilde{\Pi}$. As for its running time, $\mathsf{D}^{(0)}$ makes at most $\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil$ calls to $\mathsf{HonContSL}_{\widetilde{\Pi}}$. Every time $\mathsf{HonContSL}_{\widetilde{\Pi}}$ is called, it makes at most m calls to Est and to HC. Let $c > 0$ be a constant such that the operations $\mathsf{D}^{(0)}$ makes other than calling Est or HC take at most $c \cdot m$ steps per such call.[56] Hence, the running time of $\mathsf{D}^{(0)}$ is at most $c \cdot m^2 \cdot \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}})$.

Assume the lemma holds for $k-1$, namely, that there exists a sequence of algorithms $\{\mathsf{D}^{(i)}\}_{i \in (k-1)}$ such that $\mathsf{D}^{(i)}$ is a (ξ,δ)-biased continuator for $\widetilde{\Pi}^{(i)} = (\mathsf{A}_{\mathsf{D}^{(i-1)}}^{(i,\xi,\delta)}, \widetilde{\mathsf{B}})$[57] and $\mathsf{D}^{(k-1)}$'s running time is at most $c^k \cdot m^{2k} \cdot \lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \rceil^k \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}})$. Define

$$\mathsf{D}^{(k)} = \mathsf{BiasedCont}_\Pi^{(\xi,\delta,\mathsf{HonContSL}_{\widetilde{\Pi}^{(k)}})}.$$

Note that $\widetilde{\Pi}^{(k)}$ is stateless: $\mathsf{A}_{\mathsf{D}^{(k-1)}}^{(k,\xi,\delta)}$ simply makes calls to $\mathsf{D}^{(k-1)}$ and thus is stateless, and $\widetilde{\mathsf{B}}$ is stateless by definition. As in the base case, Claims 4.41 and 4.44 yield that $\mathsf{D}^{(k)}$ is a (ξ,δ)-biased continuator for $\widetilde{\Pi}^{(k)}$. As for the running time of $\mathsf{D}^{(k)}$, the analysis is identical to the base case, but $\mathsf{HonContSL}_{\widetilde{\Pi}^{(k)}}$ makes at most m calls to $\mathsf{D}^{(k-1)}$, HC, or Est. Since the assumed bound on the

[56] Since the input length to $\mathsf{D}^{(0)}$ is at most m, it is easy to verify that such c exists.

[57] Recall that $\mathsf{A}_{\mathsf{D}^{(i-1)}}^{(i,\xi,\delta)}$ was defined in Definition 4.35.

running time of $\mathsf{D}^{(k-1)}$ is much longer than T_{HC} and T_{Est}, the running time of $\mathsf{D}^{(k)}$ is at most

$$c \cdot m^2 \cdot \left\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \right\rceil \cdot \left(c^k \cdot m^{2k} \cdot \left\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \right\rceil^k \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}}) \right)$$
$$= c^{k+1} \cdot m^{2(k+1)} \cdot \left\lceil \frac{\log(1/\xi)}{\log(1/(1-\delta))} \right\rceil^{k+1} \cdot (T_{\mathsf{Est}} + T_{\mathsf{HC}}). \qquad \square$$

4.4.2 Implementing Estimator Using Honest Continuator—Proving Lemma 4.37. Turning an honest continuator into a *randomized* estimator is straightforward: given a transcript u, sample many honest continuations from u and return the mean of the parties' common outcome bit of these continuations.

Algorithm 4.45 ($\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$).

Parameters: $\xi \in (0,1)$.
Oracle: algorithm HC.
Input: transcript $u \in \mathcal{V}(\Pi)$.
Operation:

```
(1) Set sum = 0 and s = $\lceil \frac{\ln(2^m/\xi)}{\xi^2/2} \rceil$.
(2) For i = 1 to s: sum = sum + $\chi_{\Pi}(\mathsf{HC}(u))$.
    (each call to HC is with fresh random coins).
(3) Return sum/s.
```

The number of calls $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$ makes to HC is set so that for most choices of its coins, $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$ returns a good estimation for the value of *every* node. Thus, fixing, at random, the coins of $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$ results with high probability in a good *deterministic* estimator.

Proof of Lemma 4.37. The running time of $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$ follows immediately from its definition.[58] In the rest of the proof, we show that Item 1 holds, namely, that with probability at least $1-\xi$ over fixing its coins at random, $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$ is a ξ-estimator for Π.

Let $\mathsf{Est}_r = \mathsf{Est}_{\Pi,r}^{(\xi,\mathsf{HC})}$, let $\mu_u = \mathrm{E}_{\ell \leftarrow \mathsf{HC}(u)}[\chi(\ell)]$, and let Q_r denote the event that $\forall u \in \mathcal{V}(\Pi) \setminus \mathcal{L}(\Pi)$, and it holds that a$|\mathsf{Est}_r(u) - \mu_u| \le \xi/2$. The proof is an immediate conclusion from the following two simple observations.

(1) Condition on Q_r occurring, Est_r is a ξ-estimator for Π.
(2) $\Pr_{r \leftarrow \{0,1\}^\ell}[\neg Q_r] \le \xi$.

Proof of (1): Compute

$$\Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \left|\mathsf{Est}_r(\ell_{1,\ldots,i}) - \mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right| > \xi\right] \tag{96}$$
$$\le \Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \left|\mathsf{Est}_r(\ell_{1,\ldots,i}) - \mu_{\ell_{1,\ldots,i}}\right| > \xi/2 \vee \left|\mu_{\ell_{1,\ldots,i}} - \mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right| > \xi/2\right]$$
$$\le \Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \left|\mathsf{Est}_r(\ell_{1,\ldots,i}) - \mu_{\ell_{1,\ldots,i}}\right| > \xi/2\right]$$
$$+ \Pr_{\ell \leftarrow \langle \Pi \rangle}\left[\exists i \in (m-1) : \left|\mu_{\ell_{1,\ldots,i}} - \mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right| > \xi/2\right].$$

Since, by assumption, Q_r occurs, the first summand of the right-hand side of Equation (96) is zero. Furthermore, since HC is a $\xi/2$-honest continuator for Π, we bound the second summand of the

[58] $\mathsf{Est}_{\Pi}^{(\xi,\mathsf{HC})}$'s input length is at most m, so it makes at most $O(m)$ steps per call to HC.

right-hand side of Equation (96):

$$\begin{aligned}&\Pr_{\ell\leftarrow\langle\Pi\rangle}\left[\exists i\in(m-1):\left|\mu_{\ell_{1,\ldots,i}}-\mathsf{val}(\Pi_{\ell_{1,\ldots,i}})\right|>\xi/2\right]\\&\quad\le\Pr_{\ell\leftarrow\langle\Pi\rangle}[\exists i\in(m-1):\mathsf{SD}(\mathsf{HC}(\ell_{1,\ldots,i}),\mathsf{HonCont}_{\Pi}(\ell_{1,\ldots,i}))>\xi/2]\\&\quad\le\xi/2\le\xi.\end{aligned}$$

Plugging the above into Equation (96) completes the proof.

Proof of (2): We use the following fact derived from Hoeffding's bound.

Fact 4.46 (Sampling). *Let* $t\ge\frac{\ln(\frac{2}{\gamma})}{2\cdot\varepsilon^2}$, *let* $X_1,\ldots,X_t\in[0,1]$ *be iid Boolean random variables, and let* $\mu=\mathrm{E}[X_i]$. *Then* $\Pr[|\frac{1}{t}\sum_{i=1}^{t}X_i-\mu|\ge\varepsilon]\le\gamma$.

Taking $\varepsilon:=\xi/2$ and $\gamma:=\xi/2^m$ with Fact 4.46 yields that

$$\Pr_{r\leftarrow\{0,1\}^{\ell}}[|\mathsf{Est}_r(u)-\mu_u|>\xi/2]\le\frac{\xi}{2^m}\tag{97}$$

for every $u\in\mathcal{V}(\Pi)\setminus\mathcal{L}(\Pi)$, and a union bound yields that

$$\begin{aligned}\Pr_{r\leftarrow\{0,1\}^{\ell}}[\neg Q_r]&=\Pr_{r\leftarrow\{0,1\}^{\ell}}[\exists u\in\mathcal{V}(\Pi)\setminus\mathcal{L}(\Pi):|\mathsf{Est}_r(u)-\mu_u|>\xi/2]\\&\le\sum_{u\in\mathcal{V}(\Pi)\setminus\mathcal{L}(\Pi)}\Pr_{r\leftarrow\{0,1\}^{\ell}}[|\mathsf{Est}_r(u)-\mu_u|>\xi/2]\\&\le\sum_{u\in\mathcal{V}(\Pi)\setminus\mathcal{L}(\Pi)}\frac{\xi}{2^m}=\xi.\end{aligned}$$

□

4.5 Main Theorem—Inexistence of OWFs Implies an Efficient Attacker

We are finally ready to state and prove our main result—the existence of any constant bias (even weak) coin-flipping protocol implies the existence of one-way functions.

In the following, we consider both protocols and algorithms that get a security parameter, written in unary, as input (sometimes, in addition to other input), and protocols and algorithms that do not get a security parameter, as we did in previous sections. We refer to the former type as parameterized and to the latter type as nonparameterized. It will be clear from the context whether we consider a parameterized or nonparameterized entity. In particular, a poly-time entity whose running time is measured as a function of its security parameter is by definition parameterized. Given a parameterized protocol Π and $n\in\mathbb{N}$, let Π_n be its nonparameterized variant with the security parameter 1^n hardwired into the parties' code. We apply similar notation also for parameterized algorithms.

Theorem 4.47 (Main Theorem, Restatement of Theorem 1.1). *Assume one-way functions do not exist. For every* PPT *coin-flipping protocol* $\Pi=(\mathsf{A},\mathsf{B})$ *and* $\varepsilon>0$, *there exist* PPTMs $\mathcal{A}$ *and* $\mathcal{B}$ *such that the following hold for infinitely many n's:*

(1) $\Pr[\mathrm{out}(\mathcal{A}(1),\mathsf{B})(1^n)=1]\ge1-\varepsilon$ *or* $\Pr[\mathrm{out}(\mathsf{A},\mathcal{B}(0))(1^n)=0]\le\varepsilon$, *and*
(2) $\Pr[\mathrm{out}(\mathcal{A}(0),\mathsf{B})(1^n)=0]\le\varepsilon$ *or* $\Pr[\mathrm{out}(\mathsf{A},\mathcal{B}(1))(1^n)=1]\ge1-\varepsilon$.

The proof of Theorem 4.47 follows from Theorem 3.3 and Lemma 4.39 together with the following lemma that shows how to implement an efficient honest continuator assuming OWFs do not exist.

Lemma 4.48. *Assume one-way functions do not exist. Then for any* PPT *coin-flipping protocol* $\Pi=(\mathsf{A},\mathsf{B})$ *and* $p\in\mathrm{poly}$, *there exists a* PPTM *algorithm* HC *such that* HC_n *is a* $1/p(n)$*-honest continuator for* Π_n *for infinitely many n's.*

The proof of Lemma 4.48 is given below, but first we use it to prove Theorem 4.47.

Proving Theorem 4.47.

Proof of Theorem 4.47. We focus on proving the first part of the theorem, where the second, symmetric, part follows the same arguments.

Let $\delta = \varepsilon/8$, let $m(n) = \mathrm{round}(\Pi_n)$, and let $\xi(n) = 1/p(n) < \frac{(2\delta)^2}{16m(n)^2}$ for some large enough $p \in \mathrm{poly}$ to be determined by the analysis. Let HC be the algorithm guaranteed by Lemma 4.48, such that HC_n is a $\xi(n)/2$-honest continuator for Π_n for every n in an infinite set $\mathcal{I} \subseteq \mathbb{N}$. For $n \in \mathcal{I}$, let $\delta'_n \in [\delta/2, \delta]$ be such that $\mathrm{border}_{\Pi_n}(2\delta'_n, \xi(n)) \leq m(n) \cdot \sqrt{2\xi(n)}$, guaranteed to exist from Lemma 4.26.[59] Let $\widetilde{\Pi}_n = (\widetilde{\mathsf{A}}_n, \widetilde{\mathsf{B}}_n) = {\Pi_n}^{[2\delta'_n, \xi]}$ be the $(2\delta'_n, \xi)$-approximately pruned variant of Π_n. Let $\kappa = \kappa(\varepsilon/2)$ be such that $\mathrm{val}(\mathsf{A}^{(k)}_{\widetilde{\Pi}_n}, \widetilde{\mathsf{B}}_n) > 1 - \varepsilon/2$ or $\mathrm{val}(\widetilde{\mathsf{A}}_n, \mathsf{B}^{(k)}_{\widetilde{\Pi}_n}) < \varepsilon/2$, guaranteed to exist for every $n \in \mathcal{I}$ from Theorem 3.3. Assume without loss of generality that there exists an infinite set $\mathcal{I}' \subseteq \mathcal{I}$ such that

$$\mathrm{val}\left(\mathsf{A}^{(k)}_{\widetilde{\Pi}_n}, \widetilde{\mathsf{B}}_n\right) > 1 - \varepsilon/2 \tag{98}$$

for every $n \in \mathcal{I}'$ and let $\mu(n) = 1/n$.

Let $r, s \in \mathrm{poly}$ such that the following two equations hold:

$$\begin{aligned}
&\phi^{\mathsf{Bal}}_{k,\delta/2}\left(\mathrm{border}_{\Pi_n}(2\delta'_n, \xi(n)) + 12 \cdot m(n) \cdot \xi(n)/\delta'_n, 2\sqrt{\xi(n)}, 2 \cdot m(n) \cdot \xi(n), m(n), \delta'_n, \mu(n)\right)\\
&= \Big(\mathrm{border}_{\Pi_n}(2\delta'_n, \xi(n)) + 12 \cdot m(n) \cdot \xi(n)/\delta'_n\\
&\quad + 2\sqrt{\xi(n)}2 \cdot m(n) \cdot \xi(n)\Big) \cdot q_{\kappa,\delta/2}(m(n), 1/\delta'_n, 1/\mu(n)) + 1/\mu(n)\\
&\leq \sqrt{\xi(n)} \cdot r(n),
\end{aligned}$$

and

$$\begin{aligned}
&\phi^{\mathsf{It}}_{\kappa,\delta/2}(\mathrm{border}_{\Pi_n}(2\delta'_n, \xi(n)) + 12 \cdot m(n) \cdot \xi(n)/\delta'_n, \xi(n), m(n), \delta'_n, \mu(n))\\
&\quad = (\mathrm{border}_{\Pi_n}(2\delta'_n, \xi(n)) + 12 \cdot m(n) \cdot \xi(n)/\delta'_n + \xi(n)) \cdot p_{\kappa,\delta/2}(m(n), 1/\delta'_n, 1/\mu(n)) + 1/\mu(n)\\
&\quad \leq \sqrt{\xi(n)} \cdot s(n).
\end{aligned}$$

Note that by the setting of parameters thus far, such r and s exists. Finally, let $\xi \in \mathrm{poly}$ be such that

$$(m(n) + 2) \cdot \sqrt{\xi(n)} + \xi(n) + 2 \cdot \sqrt{\xi(n)} \cdot r(n) + 3 \cdot \sqrt{\xi(n)} \cdot s(n) \in o(1).$$

By Lemma 4.39(1),

$$\mathrm{val}\left(\widetilde{\mathsf{A}}^{(\kappa, \xi(n), \delta'_n, \mathsf{HC}_n)}_{\Pi_n}, \mathsf{B}_{\Pi_n}\right) \geq \mathrm{val}\left(\mathsf{A}^{(k)}_{\widetilde{\Pi}_n}, \widetilde{\mathsf{B}}_n\right) - 2\delta' - o(1) \geq 1 - \frac{\varepsilon}{2} - \frac{\varepsilon}{4} - o(1). \tag{99}$$

We can now define the final adversary $\mathcal{A}(1)$ that will take the role of A and bias the protocol (A, B) toward one. Let $\mathcal{V} = \{(\delta + j \cdot 2\xi)/2 : j \in \{0, 1, \ldots, \lceil m/\sqrt{\xi} \rceil\}\}$ be the set from Lemma 4.26 and recall that $\delta'_n \in \mathcal{V}$. Prior to interacting with B, algorithm $\mathcal{A}(1)$ estimates the value of $\widetilde{\Pi}_{\delta'} := (\widetilde{\mathsf{A}}^{(\kappa, \xi(n), \delta', \mathsf{HC}_n)}_{\Pi_n}, \mathsf{B}_{\Pi_n})$, for every $\delta' \in \mathcal{V}$, by running the latter protocol for polynomially many

[59] By the choice of ξ and by Lemma 4.26, there exists $\delta'' \in [\delta, 2\delta]$ such that $\mathrm{border}_{\Pi_n}(\delta'', \xi(n)) \leq m(n) \cdot \sqrt{2\xi(n)}$. Now we can set $\delta' = \delta''/2$.

times. Let δ_n^* be the value such that $\widetilde{\Pi}_{\delta_n^*}$ is the maximum of all estimations. When interacting with B, algorithm $\mathcal{A}(1)$ behaves as $\widetilde{\mathsf{A}}_{\Pi_n}^{(\kappa,\xi,\delta_n^*,\mathsf{HC}_n)}$.

Since $\delta'_n \in \mathcal{V}$, it follows that $\Pr[\mathsf{val}(\widetilde{\Pi}_{\delta_n^*}) \geq \mathsf{val}(\widetilde{\Pi}_{\delta'_n}) - \varepsilon/8] \geq 1 - o(1)$, where the probability is over the coins on $\mathcal{A}(1)$. Thus,

$$\begin{aligned}
&\Pr[\mathrm{out}(\mathcal{A}(1),\mathrm{B})(1^n) = 1] \qquad\qquad (100)\\
&\quad\geq \Pr\left[\mathrm{out}(\mathcal{A}(1),\mathrm{B})(1^n) = 1 \;\middle|\; \mathsf{val}\left(\widetilde{\Pi}_{\delta_n^*}\right) \geq \mathsf{val}\left(\widetilde{\Pi}_{\delta'_n}\right) - \varepsilon/8\right] \cdot \Pr\left[\mathsf{val}\left(\widetilde{\Pi}_{\delta_n^*}\right) \geq \mathsf{val}\left(\widetilde{\Pi}_{\delta'_n}\right) - \varepsilon/8\right]\\
&\quad\geq (1 - 5\varepsilon/8 - o(1)) \cdot (1 - o(1))\\
&\quad\geq 1 - 5\varepsilon/8 - o(1) \geq 1 - \varepsilon,
\end{aligned}$$

for large enough $n \in \mathcal{I}'$.

The last step is to argue that $\mathcal{A}(1)$ is efficient. By our choice of parameters, the fact that κ is constant (i.e., independent of n), and HC is PPTM, Lemma 4.39(2) yields that $\widetilde{\mathsf{A}}_{\Pi_n}^{(\kappa,\xi(n),\delta'_n,\mathsf{HC}_n)}$ is a PPTM. Since $|\mathcal{V}| \in \mathrm{poly}(n)$, it follows that the running time of $\mathcal{A}(1)$ is also is $\mathrm{poly}(n)$. □

It is left to prove Lemma 4.48.

Proving Lemma 4.48.

Proof of Lemma 4.48. Let $m(n) = \mathrm{round}(\Pi_n)$, and let $\rho_{\mathrm{A}}(n)$ and $\rho_{\mathrm{B}}(n)$ be, respectively, the (maximal) number of random bits used by A and B on common input 1^n. Consider the *transcript function* f_Π over $1^* \times \{0,1\}^{\rho_{\mathrm{A}}(n)} \times \{0,1\}^{\rho_{\mathrm{B}}(n)} \times (m(n)-1)$, defined by

$$f_\Pi(1^n, r_{\mathrm{A}}, r_{\mathrm{B}}, i) = 1^n, \mathrm{trans}((\mathsf{A}(\cdot; r_{\mathrm{A}}), \mathsf{B}(\cdot; r_{\mathrm{B}}))(1^n))_{1,\ldots,i}. \qquad (101)$$

Since Π is a polynomial-time protocol, it follows without loss of generality that $m(n)$, $\rho_{\mathrm{A}}(n), \rho_{\mathrm{B}}(n) \in \mathrm{poly}(n)$ and that f_Π is computable in polynomial time.

Under the assumption that OWFs do not exist, the transcript function is not distributional one-way; i.e., it has an inverter that returns a random preimage. We would like to argue that an algorithm that outputs the transcript induced by the randomness this inverter returns is an honest continuator. This is almost true, as this inverter is guaranteed to work for a random node of the protocol tree, and we require that an honest continuator work for all nodes in a random *path* of the protocol tree. Still, since any path in the protocol tree is of polynomial length, the lemma follows by a union bound. We now move to the formal proof.

Fix $p \in \mathrm{poly}$ and let Inv be the $1/(m \cdot p)$-inverter guaranteed to exist by Lemma 2.15. Namely, $\mathsf{Inv}_n = \mathsf{Inv}(1^n, \cdot)$ is a $1/(m(n) \cdot p(n))$-inverter for $f_\Pi(1^n, \cdot, \cdot, \cdot)$ for every n within an infinite size index set $\mathcal{I} \subseteq \mathbb{N}$.[60] By the definition of f_Π, choosing a random preimage from $f_\Pi^{-1}(1^n, u)$ is equivalent to choosing an element according to the distribution $(\mathrm{Consis}_{\Pi_n}(u), |u|)$.[61] For a transcript u and coins r_{A} and r_{B} for A and B, respectively, let $f_u(r_{\mathrm{A}}, r_{\mathrm{B}}, \cdot) := u \circ (\mathrm{trans}(\mathsf{A}(\cdot; r_{\mathrm{A}}), \mathsf{B}(\cdot; r_{\mathrm{B}}))(1^n))_{|u|+1,\ldots,m(n)}$, and let HC_n be the algorithm that, given input u, returns $f_u(\mathsf{Inv}_n(u))$.[62] We show that HC_n is a $1/p(n)$-honest continuator for Π_n, for every $n \in \mathcal{I}$.

[60] Lemma 2.15 is stated for functions whose domain is $\{0,1\}^n$ for every $n \in \mathbb{N}$, i.e., functions defined for every input length. Although the transcript function is not defined for every input length (and has 1^n as an input), using the fact that it is defined on $\{0,1\}^{q(n)}$ for some $q(n) \in \mathrm{poly}(n)$ and standard padding techniques, Lemma 2.15 does in fact guarantee such an inverter.

[61] Recall that $\mathrm{Consis}_\Pi(u)$ returns random coins for the parties, consistent with a random execution of Π leading to u.

[62] The function f actually ignores its third argument. It is defined to take three arguments only to match the number of arguments in the output of Inv_n.

Fix $n \in \mathcal{I}$. Let $m = m(n)$ and $p = p(n)$ and from now on we omit n from notations. Note that $f_u(\mathsf{Consis}_\Pi(u), |u|) \equiv \langle \Pi_u \rangle \equiv \mathsf{HonCont}_\Pi(u)$, and thus

$$\mathsf{SD}(\mathsf{Inv}(u), (\mathsf{Consis}_\Pi(u), |u|)) \geq \mathsf{SD}(\mathsf{HC}(u), \mathsf{HonCont}_\Pi(u)), \tag{102}$$

for every transcript u. Let I and L be random variables distributed as $I \leftarrow (m-1)$ and $L \leftarrow \langle \Pi \rangle$, respectively. Compute

$$\begin{aligned}
&\Pr\left[\mathsf{SD}(\mathsf{Inv}(L_{1,\ldots,I}), (\mathsf{Consis}_\Pi(L_{1,\ldots,I}), I)) > \frac{1}{m \cdot p}\right] \\
&= \sum_{j=0}^{m-1} \Pr\left[\mathsf{SD}(\mathsf{Inv}(L_{1,\ldots,I}), (\mathsf{Consis}_\Pi(L_{1,\ldots,I}), I)) > \frac{1}{m \cdot p} \mid I = j\right] \cdot \Pr[I = j] \\
&= \frac{1}{m} \sum_{j=0}^{m-1} \Pr\left[\mathsf{SD}\Big(\mathsf{Inv}(L_{1,\ldots,j}), \Big(\mathsf{Consis}_\Pi(L_{1,\ldots,j}), j\Big)\Big) > \frac{1}{m \cdot p}\right] \\
&\geq \frac{1}{m} \sum_{j=0}^{m-1} \Pr\left[\mathsf{SD}\Big(\mathsf{HC}(L_{1,\ldots,j}), \mathsf{HonCont}_\Pi(L_{1,\ldots,j})\Big) > \frac{1}{m \cdot p}\right] \\
&\geq \frac{1}{m} \sum_{j=0}^{m-1} \Pr\left[\mathsf{SD}\Big(\mathsf{HC}(L_{1,\ldots,j}), \mathsf{HonCont}_\Pi(L_{1,\ldots,j})\Big) > \frac{1}{p}\right] \\
&\geq \frac{1}{m} \Pr\left[\exists j \in (m-1) : \mathsf{SD}\Big(\mathsf{HC}(L_{1,\ldots,j}), \mathsf{HonCont}_\Pi(L_{1,\ldots,j})\Big) > \frac{1}{p}\right].
\end{aligned}$$

The proof now follows by the properties of Inv. □

APPENDIX

A MISSING PROOFS

A.1 Proving Lemma 2.20

Lemma A.1 (Restatement of Lemma 2.20). *Let $x, y \in [0,1]$, let $k \geq 1$ be an integer, and let $a_1, \ldots, a_k, b_1, \ldots, b_k \in (0,1]$. Then for any $p_0, p_1 \geq 0$ with $p_0 + p_1 = 1$, it holds that*

$$p_0 \cdot \frac{x^{k+1}}{\prod_{i=1}^k a_i} + p_1 \cdot \frac{y^{k+1}}{\prod_{i=1}^k b_i} \geq \frac{(p_0 x + p_1 y)^{k+1}}{\prod_{i=1}^k (p_0 a_i + p_1 b_i)}. \tag{103}$$

Proof. The lemma easily follows if one of the following holds: (1) $p_0 = 1, p_1 = 0$; (2) $p_0 = 0, p_1 = 1$; and (3) $x = y = 0$. Assuming $1 > p_0, p_1 > 0$, and $x + y > 0$, dividing Equation (103) by its right-hand side (which is always positive) gives

$$p_0 \cdot \frac{\left(\frac{x}{(p_0 x + p_1 y)}\right)^{k+1}}{\prod_{i=1}^k \frac{a_i}{p_0 a_i + p_1 b_i}} + p_1 \cdot \frac{\left(\frac{y}{(p_0 x + p_1 y)}\right)^{k+1}}{\prod_{i=1}^k \frac{b_i}{p_0 a_i + p_1 b_i}} \geq 1. \tag{104}$$

Define the following variable changes:

$$z = \frac{p_0 x}{p_0 x + p_1 y} \qquad c_i = \frac{p_0 a_i}{p_0 a_i + p_1 b_i} \quad \text{for } 1 \leq i \leq k.$$

It follows that

$$1 - z = \frac{p_1 y}{p_0 x + p_1 y} \qquad 1 - c_i = \frac{p_1 b_i}{p_0 a_i + p_1 b_i} \quad \text{for } 1 \leq i \leq k.$$

Note that $0 \leq z \leq 1$ and that $0 < c_i < 1$ for every $1 \leq i \leq k$. Plugging the above into Equation (104), it remains to show that

$$\frac{z^{k+1}}{\prod_{i=1}^{k} c_i} + \frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)} \geq 1 \tag{105}$$

for all $0 \leq z \leq 1$ and $0 < c_i < 1$. Equation (105) immediately follows for $z = 0, 1$, and in the rest of the proof we show that it also holds for $z \in (0,1)$. Define $f(z, c_1, \ldots, c_k) := \frac{z^{k+1}}{\prod_{i=1}^{k} c_i} + \frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)} - 1$. Equation (105) follows by showing that $f(z, c_1, \ldots, c_k) \geq 0$ for all $z \in (0,1)$ and $0 < c_i < 1$. Taking the partial derivative with respect to c_i for $1 \leq i \leq k$, it holds that

$$\frac{\partial}{\partial c_i} f = -\frac{z^{k+1}}{c_i^2 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} c_j} + \frac{(1-z)^{k+1}}{(1-c_i)^2 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} (1-c_j)}.$$

Fix $0 < z < 1$, and let $f_z(c_1, \ldots, c_k) = f(z, c_1, \ldots, c_k)$. If $c_1 = \cdots = c_k = z$, then for every $1 \leq i \leq k$ it holds that $\frac{\partial}{\partial c_i} f_z(c_1, \ldots, c_k) = \frac{\partial}{\partial c_i} f(z, c_1, \ldots, c_k) = 0$. Hence, f_z has a local extremum at $(c_1, \ldots, c_k) = (z, \ldots, z)$. Taking the second partial derivative with respect to c_i for $1 \leq i \leq k$, it holds that

$$\frac{\partial^2}{\partial c_i} f = \frac{2z^{k+1}}{c_i^3 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} c_j} + \frac{2(1-z)^{k+1}}{(1-c_i)^3 \prod_{\substack{1 \leq j \leq k \\ j \neq i}} (1-c_j)} > 0,$$

and thus, $(c_1, \ldots, c_k) = (z, \ldots, z)$ is a local minimum of f_z.

The next step is to show that $(c_1, \ldots, c_k) = (z, \ldots, z)$ is a global minimum of f_z. This is done by showing that f_z is convex when $0 < c_i < 1$. Indeed, consider the function $-\ln(x)$. This is a convex function for $0 < x < 1$. Thus, the function $\sum_{i=1}^{k} - \ln(c_i)$, which is a sum of convex functions, is also convex. Moreover, consider the function e^x. This is a convex function for any x. Hence, the function $e^{\sum_{i=1}^{k} - \ln(c_i)} = \frac{1}{\prod_{i=1}^{k} c_i}$, which is a composition of two convex functions, is also convex for $0 < c_i < 1$. Since z is fixed, the function $\frac{z^{k+1}}{\prod_{i=1}^{k} c_i}$ is also convex. A similar argument shows that $\frac{(1-z)^{k+1}}{\prod_{i=1}^{k}(1-c_i)}$ is also convex for $0 < c_i < 1$. This yields that f_z, which is a sum of two convex functions, is convex. It is known that a local minimum of a convex function is also a global minimum for that function [23, Theorem A, Chapter V], and thus $(z, \ldots, z)$ is a global minimum of f_z.

Let $z', c'_1, \ldots, c'_k \in (0,1)$. Since $(z', \ldots, z')$ is a global minimum of $f_{z'}$, it holds that $f(z', z', \ldots, z') = f_{z'}(z', \ldots, z') \leq f_{z'}(c'_1, \ldots, c'_k) = f(z', c'_1, \ldots, c'_k)$. But $f(z', z', \ldots, z') = 0$, and thus $f(z', c'_1, \ldots, c'_k) \geq 0$. This shows that Equation (105) holds, and the proof is concluded. □

A.2 Proving Lemma 2.21

Lemma A.2 (Restatement of Lemma 2.21). *For every $\delta \in (0, \frac{1}{2}]$, there exists $\alpha = \alpha(\delta) \in (0,1]$ such that*

$$\lambda \cdot a_1^{1+\alpha} \cdot (2 - a_1 \cdot x) + a_2^{1+\alpha} \cdot (2 - a_2 \cdot x) \leq (1+\lambda) \cdot (2-x) \tag{106}$$

for every $x \geq \delta$ and $\lambda, y \geq 0$ with $\lambda y \leq 1$, for $a_1 = 1 + y$ and $a_2 = 1 - \lambda y$.

Proof. Fix $\delta \in (0, \frac{1}{2}]$. Rearranging the terms of Equation (106), one can equivalently prove that for some $\alpha \in (0,1]$, it holds that

$$x \cdot (1 + \lambda - \lambda \cdot (1+y)^{2+\alpha} - (1-\lambda y)^{2+\alpha}) \leq 2 \cdot (1 + \lambda - \lambda \cdot (1+y)^{1+\alpha} - (1-\lambda y)^{1+\alpha}) \tag{107}$$

for all x, λ, and y in the proper range. Note that the above trivially holds, regardless of the choice of $\alpha \in (0, 1]$, if $\lambda y = 0$ (both sides of the inequality are 0). In the following, we show that for the cases $\lambda y = 1$ and $\lambda y \in (0, 1)$, Equation (107) holds for any small enough choice of α. Hence, the proof follows by taking the small enough α for which the above cases hold simultaneously.

$\lambda y = 1$: Let $z = \frac{1}{\lambda} + 1 = y + 1 > 1$. Plugging in Equation (107), we need to find $\alpha_h \in (0, 1]$ for which it holds that

$$x \cdot \left(1 + \frac{1}{z-1} - \frac{z^{2+\alpha}}{z-1}\right) \leq 2 \cdot \left(1 + \frac{1}{z-1} - \frac{z^{1+\alpha}}{z-1}\right) \tag{108}$$

for all $z > 1$ and $\alpha \in (0, \alpha_h)$. Equivalently, by multiplying both sides by $\frac{z-1}{z}$—which, since $z > 1$, is always positive—it suffices to find $\alpha_h \in (0, 1]$ for which it holds that

$$x \cdot (1 - z^{1+\alpha}) \leq 2 \cdot (1 - z^{\alpha}) \tag{109}$$

for all $z > 1$ and $\alpha \in (0, \alpha_h)$.

Since $1 - z^{1+\alpha} < 0$ for all $\alpha \geq 0$ and $z > 1$, and letting $h_\alpha(z) := \frac{z^\alpha - 1}{z^{1+\alpha} - 1}$, proving Equation (109) is equivalent to finding $\alpha_h \in (0, 1]$ such that

$$\delta \geq \sup_{z>1}\{2 \cdot h_\alpha(z)\} = 2 \cdot \sup_{z>1}\{h_\alpha(z)\} \tag{110}$$

for all $z > 1$ and $\alpha \in (0, \alpha_h)$.

Consider the function

$$h(w) := \sup_{z>1}\{h_w(z)\}. \tag{111}$$

Claim A.3 states that $\lim_{w \to 0^+} h(w) = 0$ (i.e., $h(w)$ approaches 0 when w approaches 0 from the positive side), and hence $2 \cdot \lim_{w \to 0^+} h(w) = 0$. The proof of Equation (110), and thus the proof of this part, follows since there is now small enough $\alpha_h < 1$ for which $x \geq 2 \cdot h(\alpha)$ for every $\alpha \in (0, \alpha_h]$ and $x \geq \delta$.

$\lambda y \in (0, 1)$: Consider the function

$$g(\alpha, \lambda, y) := 1 + \lambda - \lambda \cdot (1 + y)^{2+\alpha} - (1 - \lambda y)^{2+\alpha}. \tag{112}$$

Claim A.4 states that for $\alpha \geq 0$, the function g is negative over the given range of λ and y. This allows us to complete the proof by finding $\alpha \in (0, 1]$ for which

$$\delta \geq 2 \cdot \sup_{\lambda, y>0, \lambda y<1} \left\{ f_\alpha(\lambda, y) := \frac{1 + \lambda - \lambda \cdot (1 + y)^{1+\alpha} - (1 - \lambda y)^{1+\alpha}}{1 + \lambda - \lambda \cdot (1 + y)^{2+\alpha} - (1 - \lambda y)^{2+\alpha}} \right\}. \tag{113}$$

Consider the function

$$f(w) := \sup_{\lambda, y>0, \lambda y<1} \{f_w(\lambda, y)\}. \tag{114}$$

Claim A.5 states that $\lim_{w \to 0^+} h(w) = 0$, and hence $(1 + \delta) \cdot \lim_{w \to 0^+} h(w) = 0$. The proof of Equation (113), and thus the proof of this part, follows since there is now small enough $\alpha_f < 1$ for which $x \geq 2 \cdot h(\alpha)$ for every $\alpha \in (0, \alpha_f]$ and $x \geq \delta$.

By setting $\alpha_{\min} = \min\{\alpha_h, \alpha_f\}$, it follows that $x \geq h(\alpha), f(\alpha)$ for any $\alpha \in (0, \alpha_{\min})$ and $x \geq \delta$, concluding the the proof of the claim. □

Claim A.3. $\lim_{w \to 0^+} h(w) = 0$.

Proof. Simple calculations show that for fixed w, the function $h_w(z)$ is decreasing in the interval $(1, \infty)$. Indeed, fix some $w > 0$, and consider the derivative of h_w

$$\begin{aligned} h'_w(z) &= \frac{wz^{w-1}(z^{1+w} - 1) - (1+w)z^w(z^w - 1)}{(z^{1+w} - 1)^2} \\ &= \frac{-z^{w-1}(z^{1+w} - (1+w)z + w)}{(z^{1+w} - 1)^2}. \end{aligned} \tag{115}$$

Let $p(z) := z^{1+w} - (1+w)z + w$. Taking the derivative of p and equaling it to 0, we have that

$$\begin{aligned} p'(z) &= (1+w)z^w - (1+w) = 0 \\ &\iff z = 1. \end{aligned} \tag{116}$$

Since $p''(1) = (1+w)w > 0$ for all $w > 0$, it holds that $z = 1$ is the minimum of p in $[1, \infty)$. Since $p(1) = 0$, it holds that $p(a) > 0$ for every $a \in (1, \infty)$. Thus, $h'_w(z) < 0$, and $h_w(z)$ is decreasing in the interval $(1, \infty)$. The latter fact yields that

$$\begin{aligned} \lim_{w \to 0^+} h(w) &= \lim_{w \to 0^+} \sup_{z > 1} h_w(z) \\ &= \lim_{w \to 0^+} \lim_{z \to 1^+} \frac{z^w - 1}{z^{1+w} - 1} \\ &= \lim_{w \to 0^+} \lim_{z \to 1^+} \frac{wz^{w-1}}{(1+w)z^w} \\ &= \lim_{w \to 0^+} \frac{w}{1+w} \\ &= 0, \end{aligned}$$

where the third equality holds by L'Hôpital's rule. □

Claim A.4. *For all $\alpha \geq 0$ and $\lambda, y > 0$ with $\lambda y < 1$, it holds that $g(\alpha, \lambda, y) < 0$.*

Proof. Fix $\lambda, y > 0$ with $\lambda y \leq 1$ and let $f(x) := g(x, \lambda, y)$. We first prove that f is strictly decreasing in the range $[0, \infty)$, and then show that $f(0) < 0$, yielding that $g(\alpha, \lambda, y) < 0$ for the given range of parameters. Taking the derivative of f, we have that

$$f'(x) = -\lambda \cdot (1+y)^{2+x} \cdot \ln(1+y) + (1 - \lambda y)^{2+x} \cdot \ln(1 - \lambda y), \tag{117}$$

and since $\ln(1 - \lambda y) < 0$, it holds that f' is a negative function. Hence, f is strictly decreasing and takes its (unique) maximum over $[0, \infty)$ at 0. We conclude the proof by noting that $f(0) = -\lambda \cdot y^2 \cdot (1 + \lambda) < 0$. □

Claim A.5. $\lim_{w \to 0^+} f(w) = 0$.

Proof. Assume toward a contradiction that the claim does not hold. It follows that there exist $\varepsilon > 0$ and an infinite sequence $\{w_i\}_{i \in \mathbb{N}}$ such that $\lim_{i \to \infty} w_i = 0$ and $f(w_i) \geq \varepsilon$ for every $i \in \mathbb{N}$. Hence, there exists an infinite sequence of pairs $\{(\lambda_i, y_i)\}_{i \in \mathbb{N}}$ such that for every $i \in \mathbb{N}$, it holds that $f(w_i) = f_{w_i}(\lambda_i, y_i) \geq \varepsilon$, $\lambda_i, y_i > 0$ and $\lambda_i y_i \leq 1$.

If $\{\lambda_i\}_{i \in \mathbb{N}}$ is not bounded from above, we focus on a subsequence of $\{(\lambda_i, y_i)\}$ in which λ_i converges to ∞, and let $\lambda^* = \infty$. Similarly, if $\{y_i\}_{i \in \mathbb{N}}$ is not bounded from above, we focus on a subsequence of $\{(\lambda_i, y_i)\}$ in which y_i converges to ∞, and let $y^* = \infty$. Otherwise, by the Bolzano-Weierstrass Theorem, there exists a subsequence of $\{(\lambda_i, y_i)\}$ in which both λ_i and y_i converge to some real values. We let λ^* and y^* be these values.

The rest of the proof splits according to the values of λ^* and y^*. In each case, we focus on the subsequence of $\{(w_i, \lambda_i, y_i)\}$ that converges to $(0, \lambda^*, y^*)$ and show that $\lim_{i \to \infty} f_{w_i}(\lambda_i, y_i) = 0$, in contradiction to the above assumption.

$y^* = \infty$: First note that the assumption $y^* = \infty$ and the fact that $\lambda_i y_i \le 1$ for every i yield that $\lambda^* = 0$.

For $c \in [0,1)$, the Taylor expansion with Lagrange remainder over the interval $[0,c]$ yields that

$$(1-c)^t = 1 - tc + \frac{t(t-1)(1-s)^{t-2}}{2} c^2 \tag{118}$$

for some $s \in (0,c)$. Consider the function

$$g(t,\lambda,y) := 1 + \lambda - \lambda \cdot (1+y)^t - (1-\lambda y)^t. \tag{119}$$

Equation (118) yields that

$$\begin{aligned} g(t,\lambda_i,y_i) &= 1 + \lambda_i - \lambda_i \cdot (1+y_i)^t - \left(1 - t\lambda_i y_i + \frac{t(t-1)(1-s_i)^{t-2}}{2}\lambda_i^2 y_i^2\right) \\ &= \lambda_i\left(1 - (1+y_i)^t + ty - \frac{t(t-1)(1-s_i)^{t-2}}{2}\lambda_i y_i^2\right) \end{aligned} \tag{120}$$

for every index i and some $s_i \in (0, \lambda_i y_i)$. We conclude that

$$\begin{aligned} \lim_{i\to\infty} f_{w_i}(\lambda_i,y_i) &= \lim_{i\to\infty} \frac{g(1+w_i,\lambda_i,y_i)}{g(2+w_i,\lambda_i,y_i)} \\ &= \lim_{i\to\infty} \frac{1-(1+y_i)^{1+w_i} + (1+w_i)y_i - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}}{2}\lambda_i y_i^2}{1-(1+y_i)^{2+w_i} + (2+w_i)y_i - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}}{2}\lambda_i y_i^2} \\ &= \lim_{i\to\infty} \frac{\frac{1}{(1+y_i)^{2+w_i}} - \frac{(1+y_i)^{1+w_i}}{(1+y_i)^{2+w_i}} + \frac{(1+w_i)y_i}{(1+y_i)^{2+w_i}} - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}\lambda_i y_i^2}{2(1+y_i)^{2+w_i}}}{\frac{1}{(1+y_i)^{2+w_i}} - 1 + \frac{(2+w_i)y_i}{(1+y_i)^{2+w_i}} - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}\lambda_i y_i^2}{2(1+y_i)^{2+w_i}}} \\ &= 0. \end{aligned}$$

$\lambda^* = \infty$: Note that the assumption $\lambda^* = \infty$ yields that $y^* = 0$. For $c \in [0,1)$, the Taylor expansion with Lagrange remainder over the interval $[0,c]$ yields that

$$(1-c)^t = 1 - tc + \frac{t(t-1)}{2}c^2 - \frac{t(t-1)(t-2)(1-s)^{t-3}}{6}c^3 \tag{121}$$

for some $s \in (0,c)$ and

$$(1+c)^t = 1 + tc + \frac{t(t-1)}{2}c^2 + \frac{t(t-1)(t-2)(1+s')^{t-3}}{6}c^3 \tag{122}$$

for some $s' \in (0,c)$.

Applying Equations (121) and (122) for the function g of Equation (119) yields that

$$\begin{aligned} &g(t,\lambda_i,y_i) \\ &= \widetilde{g}(t,\lambda_i,y_i,s_i,s_i') \\ &:= 1 + \lambda_i - \lambda_i\left(1 + ty + \frac{t(t-1)}{2}y_i^2 + \frac{t(t-1)(t-2)(1+s_i')^{t-3}}{6}y_i^3\right) \\ &\quad - \left(1 - t\lambda_i y_i + \frac{t(t-1)}{2}\lambda_i^2 y_i^2 + \frac{t(t-1)(t-2)(1-s_i)^{t-3}}{6}\lambda_i^3 y_i^3\right) \\ &= -\frac{\lambda_i^2 y_i^2}{6}\left(\frac{3t(t-1)}{\lambda_i} + \frac{t(t-1)(t-2)(1+s_i')^{t-3}y_i}{\lambda_i} + 3t(t-1) + t(t-1)(t-2)(1-s_i)^{t-3}\lambda_i y_i\right) \end{aligned} \tag{123}$$

for large enough index i and some $s_i \in (0, \lambda_i y_i)$ and $s'_i \in (0, y_i)$. We conclude that

$$\begin{aligned}
&\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) \\
&\quad = \lim_{i\to\infty} \frac{g(1 + w_i, \lambda_i, y_i)}{g(2 + w_i, \lambda_i, y_i)} \\
&\quad = \lim_{i\to\infty} \frac{\widetilde{g}(1 + w_i, \lambda_i, y_i, s_i, s'_i)}{\widetilde{g}(2 + w_i, \lambda_i, y_i, s_i, s'_i)} \\
&\quad = \lim_{i\to\infty} \left(\frac{\frac{3(1+w_i)w_i}{\lambda_i} + \frac{(1+w_i)w_i(w_i-1)(1+s'_i)^{w_i-1} y_i}{\lambda_i} + 3(1+w_i)w_i + (1+w_i)w_i(w_i-1)(1-s_i)^{w_i-2}\lambda_i y_i}{\frac{3(2+w_i)(1+w_i)}{\lambda_i} + \frac{(2+w_i)(1+w_i)w_i(1+s')^{w_i-1} y_i}{\lambda_i} + 3(2+w_i)(1+w_i) + (2+w_i)(1+w_i)w_i(1-s)^{w_i-1}\lambda_i y_i} \right) \\
&\quad = \frac{0}{6} = 0,
\end{aligned}$$

where the next-to-last equality holds since $\lambda_i y_i \leq 1$ for every i, and hence the last term of the numerator and denominator goes to 0 when $i \to \infty$.

$\lambda^*, y^* > 0$: It holds that

$$\begin{aligned}
\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) &= \lim_{i\to\infty} \frac{1 + \lambda_i - \lambda_i \cdot (1 + y_i)^{1+w_i} - (1 - \lambda_i y_i)^{1+w_i}}{1 + \lambda_i - \lambda_i \cdot (1 + y_i)^{2+w_i} - (1 - \lambda_i y_i)^{2+w_i}} \\
&= \frac{1 + \lambda^* - \lambda^*(1 + y^*) - (1 - \lambda^* y^*)}{1 + \lambda^* - \lambda^*(1 + y^*)^2 - (1 - \lambda^* y^*)^2} \\
&= 0.
\end{aligned}$$

$\lambda^* = 0$ and $y^* > 0$: Equations (118) and (120) yield that

$$\begin{aligned}
\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) &= \lim_{i\to\infty} \frac{1 - (1 + y_i)^{1+w_i} + (1 + w_i)y_i - \frac{(1+w_i)w_i(1-s_i)^{w_i-1}}{2}\lambda_i y_i^2}{1 - (1 + y_i)^{2+w_i} + (2 + w_i)y_i - \frac{(2+w_i)(1+w_i)(1-s_i)^{w_i}}{2}\lambda_i y_i^2} \\
&= \frac{1 - (1 + y^*) + y^*}{1 - (1 + y^*)^2 + 2y^*} \\
&= 0.
\end{aligned}$$

$y^* = 0$: Rearranging Equation (123) yields that the following holds for large enough index i:

$$\begin{aligned}
&g(t, \lambda_i, y_i) \\
&\quad = \widetilde{g}(t, \lambda_i, y_i, s_i, s'_i) \\
&\quad = -\frac{\lambda_i y_i^2}{6}\Big(3t(t-1) + t(t-1)(t-2)(1 + s'_i)^{t-3} y_i + 3t(t-1)\lambda_i \\
&\qquad + t(t-1)(t-2)(1 - s_i)^{t-3}\lambda_i^2 y_i\Big)
\end{aligned} \tag{124}$$

for some $s_i \in (0, \lambda_i y_i)$ and $s_i \in (0, y_i)$. Given this formulation, it is easy to see that

$$\begin{aligned}
\lim_{i\to\infty} f_{w_i}(\lambda_i, y_i) &= \lim_{i\to\infty} \frac{\widetilde{g}(1 + w_i, \lambda_i, y_i, s_i, s'_i)}{\widetilde{g}(2 + w_i, \lambda_i, y_i, s_i, s'_i)} \\
&= \frac{0}{6 + 6\lambda^*} \\
&= 0.
\end{aligned}$$

The above holds since every term in the numerator goes to 0 and the term $3(2 + w_i)(1 + w_i)$ in the denominator goes to 6.

This concludes the case analysis, and thus the proof of the claim. □

ACKNOWLEDGMENTS

The authors are very grateful to Hemanta Maji, Yishay Mansour, Eran Omri and Alex Samorodnitsky for useful discussions. The authors would also like to thank the anonymous referees for their valuable comments and helpful suggestions.

REFERENCES

[1] B. Averbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. 1985. How to implement Bracha's $O(\log n)$ Byzantine agreement algorithm. Unpublished manuscript.

[2] A. Beimel, E. Omri, and I. Orlov. 2010. Protocols for multiparty coin toss with dishonest majority. In *Advances in Cryptology (CRYPTO'10)*. 538–557.

[3] I. Berman, I. Haitner, and A. Tentes. 2014. Coin flipping of *any* constant bias implies one-way functions. In *Symposium on Theory of Computing (STOC'14)*. 398–407. DOI: https://doi.org/10.1145/2591796.2591845

[4] M. Blum. 1981. Coin flipping by telephone. In *Advances in Cryptology (CRYPTO'81)*. 11–15.

[5] A. Chailloux and I. Kerenidis. 2009. Optimal quantum strong coin flipping. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS'09)*. 527–533.

[6] R. Cleve. 1986. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC'86)*. 364–369.

[7] R. Cleve and R. Impagliazzo. 1993. Martingales, collective coin flipping and discrete control processes (Extended Abstract). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.51.1797.

[8] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. 2011. On the black-box complexity of optimally-fair coin tossing. In *Theory of Cryptography, 8th Theory of Cryptography Conference (TCC'11)*, Vol. 6597. 450–467.

[9] O. Goldreich, S. Goldwasser, and S. Micali. 1984. On the cryptographic applications of random functions. In *Advances in Cryptology (CRYPTO'84)*. 276–288.

[10] O. Goldreich, S. Goldwasser, and S. Micali. 1986. How to construct random functions. *J. ACM* 33 (1986), 792–807. http://dblp.uni-trier.de/rec/bibtex/journals/jacm/GoldreichGM86.

[11] O. Goldreich and L. A. Levin. 1989. A hard-core predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC'89)*. 25–32.

[12] I. Haitner, M. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan. 2009. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.* 39, 3 (2009), 1153–1218.

[13] I. Haitner and E. Omri. 2011. Coin flipping with constant bias implies one-way functions. In *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science (FOCS'11)*. 110–119.

[14] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. 1999. A pseudorandom generator from any one-way function. *SIAM J. Comput.* 28 (1999), 1364–1396. Preliminary versions in *STOC'89* and *STOC'90*. http://dblp.uni-rier.de/rec/bibtex/journals/siamcomp/HastadILL99.

[15] R. Impagliazzo. Pseudo-random generators for cryptography and for randomized algorithms. Ph.D. Thesis. Retrieved from http://cseweb.ucsd.edu/russell/format.ps.

[16] R. Impagliazzo and M. Luby. 1989. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS'89)*. 230–235.

[17] A. Y. Kitaev. 2003. Quantum coin-flipping. (2003). Presentation at the *6th Workshop on Quantum Information Processing (QIP'03)*.

[18] H. K. Maji, M. Prabhakaran, and A. Sahai. 2010. On the computational complexity of coin flipping. In *Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS'10)*. 613–622.

[19] C. Mochon. 2007. Quantum weak coin flipping with arbitrarily small bias. *arXiv:0711.4114*. (2007).

[20] T. Moran, M. Naor, and G. Segev. 2009. An optimally fair coin toss. In *Theory of Cryptography, 6th Theory of Cryptography Conference (TCC'09)*. 1–18.

[21] M. Naor. 1991. Bit commitment using pseudorandomness. *J. Cryptol.* 4 (1991), 151–158. Preliminary version in *CRYPTO'89*. http://dblp.uni-trier.de/rec/bibtex/journals/joc/Naor91.

[22] M. Naor and M. Yung. 1989. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC'89)*. 33–43.

[23] A. Wayne Roberts and D. E. Varberg. 1973. *Convex Functions*. Academic Press.

[24] J. Rompel. 1990. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC'90)*. 387–394.

[25] S. Zachos. 1986. Probabilistic quantifiers, adversaries, and complexity classes: An overview. In *Proceedings of the 1st Annual IEEE Conference on Computational Complexity*. 383–400.

Received June 2015; revised February 2017; accepted November 2017