Lower Bounds on Round Complexity of Randomized Byzantine Agreement Protocols

Abstract

We initiate the study of lowerbounding the round complexity of *randomized* Byzantine agreement (BA) protocols, bounding the halting probability of such protocols after one and two rounds. In particular, we show that:

1. BA protocols resilient against $n/3$ [resp., $n/4$] corruptions terminate (under attack) at the end of the first round with probability at most $o(1)$ [resp., $1/2 + o(1)$].
2. BA protocols resilient against $n/4$ corruptions terminate at the end of the second round with probability at most $1 - \Theta(1)$.
3. For a large class of protocols (including all BA protocols used in practice) and under a plausible combinatorial conjecture, BA protocols resilient against $n/3$ [resp., $n/4$] corruptions terminate at the end of the second round with probability at most $o(1)$ [resp., $1/2 + o(1)$].

The above bounds hold even when the parties use a trusted setup phase, e.g., a public-key infrastructure (PKI).

The third bound essentially matches the recent protocol of Micali (ITCS'17) that tolerates up to $n/3$ corruptions and terminates at the end of the third round with constant probability.

Keywords: Byzantine agreement; lower bound; round complexity.

Contents

1 Introduction

Byzantine agreement (BA) [40, 31] is one of the most important problems in theoretical computer science. In a BA protocol, a set of n parties wish to jointly agree on one of the honest parties' input bits. The protocol is *t-resilient* if no set of t corrupted parties can collude and prevent the honest parties from completing this task. In the closely related problem of *broadcast*, all honest parties must agree on the message sent by a (potentially corrupted) sender. Byzantine agreement and broadcast are fundamental building blocks in distributed computing and cryptography, with applications in fault-tolerant distributed systems [9, 30], secure multiparty computation [44, 25, 5, 10], and more recently, cryptocurrencies [11, 24, 39].

In this work we consider the *synchronous* communication model, where the protocol proceeds in rounds. It is well known that in the plain model, without any trusted setup assumptions, BA and broadcast can be solved if and only if $t < n/3$ [40, 31, 19, 22]. Assuming the existence of digital signatures and a public-key infrastructure (PKI), BA can be solved in the honest-majority setting $t < n/2$, and broadcast under any number of corruptions $t < n$ [15]. Information-theoretic variants that remain secure against computationally unbounded adversaries exist using information-theoretic pseudo-signatures [41].

An important aspect of BA and broadcast protocols is their *round complexity*. Deterministic t-resilient protocols require at least $t+1$ rounds [18, 15], which is a tight lower bound [15, 22]. The breakthrough results of Ben-Or [4] and Rabin [42] showed that this limitation can be circumvented using randomization. In particular, Rabin [42] used *random beacons* (common random coins that are secret-shared among the parties in a trusted setup phase) to construct a BA protocol resilient to $t < n/4$ corruptions. Rabin's protocol fails with probability 2^{-r} after r rounds, and requires *expected* constant number of rounds to reach agreement. This line of research culminated with the work of Feldman and Micali [17] who showed how to compute the common coins from scratch, yielding expected-constant-round BA protocol in the plain model, resilient to $t < n/3$ corruptions. Katz and Koo [29] gave an analogue result in the PKI-model for the honest-majority case. Recent results use trusted setup and cryptographic assumptions to establish a surprisingly small expected round complexity, namely 9 for $t < n/3$ [33] and 10 for $t < n/2$ [34, 2].

The expected-constant-round protocols mentioned above are guaranteed to terminate (with negligible error probability) within a poly-logarithmic number of rounds. The lower bounds on the guaranteed termination from [18, 15] were generalized by [12, 28], showing that any randomized r-round protocol must fail with probability at least $(c \cdot r)^{-r}$ for some constant c. However, to date there is no lower bound on the *expected* round complexity of randomized BA.

In this work, we tackle this question and show new lower bounds for randomized BA. To make the discussion more informative, we consider a more explicit definition that bounds the halting probability within a specific number of rounds. A lower bound based on such a definition readily implies a lower bound on the expected round complexity of the BA protocol.

1.1 The Model

We start with describing in more details the model in which our lower bounds are given. In the BA protocols we consider the parties are communicating over a synchronous network of private and authenticated channels. Each party starts the protocol with an input bit and upon completion decides on an output bit. The protocol is t-resilient if when facing t colluding parties that attack the protocol it holds that: (1) all honest parties agree on the same output bit (*agreement*), and (2) if all honest parties start with the same input bit, then this is the common output bit (*validity*). The protocols might have a *trusted setup phase*: a trusted external party samples correlated values and distributes them between the parties. A setup phase is known to be essential for tolerating $t \geq n/3$ corruptions, and seems to be crucial for highly efficient protocols such as [33, 11, 34, 2, 1]. The trusted setup phase is typically implemented using (heavy) secure multiparty computation [6, 8], via a public-key infrastructure, or with a random oracle (that is used to model proof of work) [38].

Locally consistent adversaries. The attacks presented in the paper require very limited capabilities from the corrupted parties (a limitation that makes our bounds stronger). Specifically they might (1) prematurely abort, and (2) send messages to different parties based on *differing* input bits and/or incoming messages from other corrupted parties. We emphasize that corrupted parties sample their random coins honestly (and use the same coins for all messages sent). In addition, they do not lie about messages received from honest parties.

Public-randomness protocols. In many randomized protocols, including all those used in practice, cryptography is merely used to provide *message authentication*—preventing a party from lying about the messages it received—and *verifiable randomness*—forcing the parties to toss their coins correctly. The description of such protocols can be greatly simplified if only security against locally consistent adversaries is required (in which corrupted parties do not lie about their coin tosses and their incoming messages from honest parties). This motivates the definition of *public-randomness* protocols, where each party publishes its local coin tosses for each round (the party's first message also contains its setup parameter, if such exists). Although our attacks apply to arbitrary BA protocols, we show even stronger lower bounds for public-randomness protocols.

We illustrate the simplicity of the model by considering the BA protocol of Micali [33]. In this protocol, the cryptographic tools, digital signatures and verifiable random functions (VRFs)[1], are used to allow the parties elect leaders and toss coins with probability $2/3$ as follows: each party P_i in round r evaluates the VRF on the pair (i, r) and multicasts the result. The leader is set to be the party with the smallest VRF value, and the coin is set to be the least-significant bit of this value. Since these values are uniformly distributed κ-bit strings (κ is the security parameter), and there are at least $2n/3$ honest parties, the success probability is $2/3$. (Indeed, with probability $1/3$, the leader is corrupted, and can send its value only to a subset of the parties, creating disagreement.)

When considering locally consistent adversaries, Micali's protocol can be significantly simplified by having each party randomly sample and multicast a uniformly distributed κ-bit string (cryptographic tools and setup phase are no longer needed). Corrupted parties can still send their values to a subset of honest parties as before, but they cannot send different random values to different honest parties.

A similar simplification applies to other BA protocols that are based on leader election and coin tosses such as [17, 20, 29] (private channels are used for a leader-election sub-protocol), [34, 2] (cryptography is used for coin-tossing and message-authentication), and [11, 1] (cryptography is used to elect a small committee per round).[2]

[1] A pseudorandom function that provides a non-interactively verifiable proof for the correctness of its output.

[2] Unlike the aforementioned protocols that use "simple" preprocess and "light-weight" cryptographic tools, the protocol of Rabin [42] uses a heavy, per execution, setup phase (consisting of Shamir sharing of a random coin for every potential round) that we do not know how to cast as a public-randomness protocol.

Proposition 1.1 (Malicious security to locally consistent public-randomness protocol, informal)**.** *Each of the BA protocols of [17, 20, 29, 33, 11, 34, 2, 1] induces a public-randomness BA protocol secure against locally consistent adversaries, with the same parameters.*

A useful abstraction for protocol design. To complete the picture, we remark that security against locally consistent adversaries, which may seem somewhat weak at first sight, can be compiled using standard cryptographic techniques into security against arbitrary adversaries. This reduction becomes lossless, efficiency-wise and security-wise, when applied to public-randomness protocols. Thus, building public-randomness protocols secure against locally consistent adversaries is a useful abstraction for protocol designers that want to use what cryptography has to offer, but without being bothered with the technical details. See more details in Appendix A.1.

1.2 Our Results

We present three lower bounds on the halting probability of randomized BA protocols. To keep the following introductory discussion simple, we will assume that both validity and agreement properties hold perfectly, without error.

First-round halting. Our first result bounds the halting probability after a single communication round. This is the simplest case since parties cannot inform each other about inconsistencies they encounter. Indeed, the established lower bound is quite strong, showing an exponentially small bound on the halting probability when $t \geq n/3$, and exponentially close to $1/2$ when $t \geq n/4$.

Theorem 1.2 (First-round halting, informal)**.** *Let Π be an n-party BA protocol and let γ denote the halting probability after a single communication round facing a locally consistent, static, adversary corrupting t parties. Then,*

- *$t \geq n/3$ implies $\gamma \leq 2^{t-n}$ for arbitrary protocols, and $\gamma = 0$ for public-randomness protocols.*
- *$t \geq n/4$ implies $\gamma \leq 1/2 + 2^{t-n}$ for arbitrary protocols, and $\gamma \leq 1/2$ for public-randomness protocols.*

Note that the deterministic $(t+1)$-round, t-resilient BA protocol of Dolev and Strong [15] can be cast as a locally consistent public-randomness protocol (in the plain model).[3] Theorem 1.2 shows that for $n = 3$ and $t = 1$, this two-round BA protocol is essentially optimal and cannot be improved via randomization (at least without considering complex protocols that cannot be cast as public-randomness protocols).

Second-round halting for arbitrary protocols. Our second result considers the halting probability after two communication rounds. This is a much more challenging regime, as honest parties have time to detect inconsistencies in first-round messages. Our bound for arbitrary protocols in this case is weaker, and shows that when $t > n/4$, the halting probability is bounded away from 1.

Theorem 1.3 (Second-round halting, arbitrary protocols, informal)**.** *Let Π be an n-party BA protocol and let γ denote the halting probability after two communication rounds facing a locally consistent, static, adversary corrupting $t = (1/4 + \varepsilon)n$ parties. Then, $\gamma \leq 1 - (\varepsilon/5)^2$.*

[3] When considering locally consistent adversaries, the impossibility of BA for $t = n/3$ does not apply.

Second-round halting for public-randomness protocols. Theorem 1.3 bounds the second-round halting probability of arbitrary BA protocols away from one. For public-randomness protocol we achieve a much stronger bound. The attack requires *adaptive* corruptions (as opposed to *static* corruptions in the previous case) and is based on a combinatorial conjecture that is stated below.[4]

Theorem 1.4 (Second-round halting, public-randomness protocols, informal). *Let Π be an n-party public-randomness BA protocol and let γ denote the halting probability after two communication rounds facing a locally consistent adversary adaptively corrupting t parties. Then, for sufficiently large n and assuming Conjecture 1.5 holds,*

- $t > n/3$ *implies* $\gamma = 0$.
- $t > n/4$ *implies* $\gamma \leq 1/2$.

Theorem 1.4 shows that for sufficiently large n, any public-randomness protocol tolerating $t > n/3$ locally consistent corruptions cannot halt in less than three rounds (unless Conjecture 1.5 is false). In particular, its expected round complexity must be at least three.

To understand the meaning of this result, recall the protocol of Micali [33]. As discussed above, this protocol can be cast as a public-randomness protocol tolerating $t < n/3$ adaptive locally consistent corruptions. The protocol proceeds by continuously running a three-round sub-protocol until halting, where each sub-protocol consists of a coin-tossing round, a check-halting-on-0 round, and a check-halting-on-1 round. Executing a single instance of this sub-protocol demonstrates a halting probability of 1/3 after three rounds. By Theorem 1.4, a protocol that tolerates slightly more corruptions, i.e., $(1/3 + \varepsilon) \cdot n$, for arbitrarily small $\varepsilon > 0$, cannot halt in fewer rounds.

Our techniques. Our attacks follow the spirit of many lower bounds on the round complexity on BA and broadcast [18, 15, 28, 16, 23, 3]. The underlying idea is to start with a configuration in which validity assures the common output is 0, and gradually adjust it, while retaining the same output value, into a configuration in which validity assures the common output is 1. (For the simple case of deterministic protocols, each step of the argument requires the corrupted parties to lie about their input bits and incoming messages from other corrupted parties, but

Our main contribution, which departs from the aforementioned paradigm, is adding another dimension to the attack by aborting a random subset of parties (rather than simply manipulating the input and incoming messages). This change allows us to bypass a seemingly inherent barrier for this approach. We refer the reader to Section 2 for a detailed overview of our attacks.

The combinatorial conjecture. We conclude the present section by motivating and stating the combinatorial conjecture assumed in Theorem 1.4, and discussing its plausibility. We believe the conjecture to be of independent interest, as it relates to topics from Boolean functions analysis such as influences of subsets of variables [37] and isoperimetric-type inequalities [35, 36]. The nature of our conjecture makes the following paragraphs somewhat technical, and reading them can be postponed until after going over the description of our attack in Section 2.

[4]The attack holds even without assuming Conjecture 1.5 when considering *strongly adaptive* corruptions [26], in which an adversary sees all messages sent by honest parties in any given round and, based on the message content, decides whether to corrupt a party (and alter its message or sabotage its delivery) or not. Similarly, the conjecture is not required if each party is limited to tossing a single unbiased coin. These extensions are not formally proved in this paper.

The analysis of our attack naturally gives rise to an isoperimetric-type inequality. For limited types of protocols, we manage to prove it using Friedgut's theorem [21] about approximate juntas and the KKL theorem [27]. For arbitrary protocols, however, we only manage to reduce our attack to the conjecture below.

We require the following notation before stating the conjecture. Let Σ denote some finite set. For $\boldsymbol{x} \in \Sigma^n$ and $\mathcal{S} \subseteq [n]$, define the vector $\perp_{\mathcal{S}}(\boldsymbol{x}) \in \{\Sigma \cup \perp\}^n$ by assigning all entries indexed by $\mathcal{S}$ with the value $\perp$, and all other entries according to $\boldsymbol{x}$. Finally, let $\mathbf{D}_{n,\sigma}$ denote the distribution induced over subsets of $[n]$ by choosing each element with probability σ independently at random.

Conjecture 1.5. *For any $\sigma, \lambda > 0$ there exists $\delta > 0$ such that the following holds for large enough $n \in \mathbb{N}$: let Σ be a finite alphabet, and let $\mathcal{A}_0, \mathcal{A}_1 \subseteq \{\Sigma \cup \perp\}^n$ be two sets such that for both $b \in \{0,1\}$:*

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} \left[\Pr_{\boldsymbol{r} \leftarrow \Sigma^n} [\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b] \geq \lambda \right] \geq 1 - \delta.$$

Then,

$$\Pr_{\substack{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma} \\ \boldsymbol{r} \leftarrow \Sigma^n}} [\forall b \in \{0,1\} \colon \{\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b \neq \emptyset] \geq \delta.$$

Consider two large sets $\mathcal{A}_0$ and $\mathcal{A}_1$ which are "stable" in the following sense: for both $b \in \{0,1\}$, with probability $1-\delta$ over $\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}$, it holds that both $\boldsymbol{r}$ and $\perp_{\mathcal{S}}(\boldsymbol{r})$ belong to $\mathcal{A}_b$, with probability at least λ over $\boldsymbol{r}$. Conjecture 1.5 stipulates that with high probability ($\geq \delta$), the vectors $\boldsymbol{r}$ and $\perp_{\mathcal{S}}(\boldsymbol{r})$ lie in opposite sets (i.e., one is in $\mathcal{A}_0$ and the other $\mathcal{A}_{1-b}$), for random $\boldsymbol{r}$ and $\mathcal{S}$. It is somewhat reminiscent of the following flavor of isoperimetric inequality: for any two large sets $\mathcal{B}_0$ and $\mathcal{B}_1$, taking a random element from $\mathcal{B}_0$ and resampling a few coordinates, yields an element in $\mathcal{B}_1$ with large probability. Less formally, one can "move" from one set to the other by manipulating a few coordinates [35, 36].

A few remarks are in order. First, it suffices for our purposes to show that δ is a noticeable (i.e., inverse polynomial) function of n, rather than independent of n.[5] We opted for the latter as it gives a stronger attack. Second, the conjecture holds for "natural" sets such as balls, i.e., $\mathcal{A}_0$ and $\mathcal{A}_1$ are balls centered around 0^n and 1^n of constant radius,[6] and "prefix" sets, i.e., sets of the form $\mathcal{A}_b = b^k \times \{\Sigma \cup \perp\}^{n-k}$. Furthermore, the claim can be proven when the probabilities over $\mathcal{S}$ and $\boldsymbol{r}$ are reversed, i.e., "with probability λ over $\boldsymbol{r}$, it holds that both $\boldsymbol{r}$ and $\perp_{\mathcal{S}}(\boldsymbol{r})$ belong to $\mathcal{A}_b$ with probability at least $1-\delta$ over $\mathcal{S}$", instead of the above. Interestingly, this weaker statement boils down to the aforementioned isoperimetric-type inequality (c.f. [35] for the Boolean case and [36] for the non Boolean case).

We conclude by pointing out that, as mentioned in Footnote 4, the conjecture is not needed for certain limited cases that are not addressed in detail in the present paper. One such case is sketched out in Section 2.

Paper Organization

In Section 2 we present a technical overview of our attacks. Due to space limitations, we differ the related work to Appendix A. The formal model and the exact bounds are stated in Appendix B. The proof of the first-round halting is given in Appendix C, and for second-round halting in Appendix D.

[5] We remark that it is rather easy to show that $\delta \geq 2^{-n}$, which is not good enough for our purposes.

[6] The alphabet Σ is not necessarily Boolean, and there are a couple of subtleties in defining balls.

2 Our Techniques

In this section, we outline our techniques for proving the lower bounds.

Notations We use calligraphic letters to denote sets, uppercase for random variables, lowercase for values, boldface for vectors, and sans-serif (e.g., A) for algorithms (i.e., Turing Machines). For $n \in \mathbb{N}$, let $[n] = \{1, \cdots, n\}$ and $(n) = \{0, 1, \cdots, n\}$. Let $\operatorname{dist}(x, y)$ denote the hamming distance between x and y. For a set $\mathcal{S} \subseteq [n]$ let $\overline{\mathcal{S}} = [n] \setminus \mathcal{S}$. For a set $\mathcal{R} \subseteq \{0,1\}^n$, let $\mathcal{R}|_{\mathcal{S}} = \{\boldsymbol{x}_{\mathcal{S}} \in \{0,1\}^{|\mathcal{S}|}$ s.t. $\boldsymbol{x} \in \mathcal{R}\}$, i.e., $\mathcal{R}|_{\mathcal{S}}$ is the projection of $\mathcal{R}$ on the index-set $\mathcal{S}$.

Fix an n-party randomized BA protocol $\Pi = (\mathsf{P}_1, \ldots, \mathsf{P}_n)$. For presentation purposes, we assume that validity and agreement hold *perfectly*, and consider no setup parameters (in the subsequent sections, we remove these assumptions). Furthermore, we only address here the case where the security threshold is $t > n/3$. The case $t > n/4$ requires an additional generic step that we defer to the technical sections of the paper. We denote by $\Pi(\boldsymbol{v}; \boldsymbol{r})$ the output of an honest execution of Π on input $\boldsymbol{v} \in \{0,1\}^n$ and randomness $\boldsymbol{r}$ (i.e., each party P_i holds input $\boldsymbol{v}_i$ and randomness $\boldsymbol{r}_i$). We let $\Pi(\boldsymbol{v})$ denote the resulting random variable determined by the parties' random coins, and we write $\Pi(\boldsymbol{v}) = b$ to denote the event that the parties output b in an honest execution of Π on input $\boldsymbol{v}$. All corrupt parties described below are locally consistent (see Section 1.1).

2.1 First-Round Halting

Assume the honest parties of Π halt after one round with probability $\gamma > 0$ when facing t corruptions. Our goal is to upperbound the value of γ. Our approach is inspired by the analogous lower-bound for deterministic protocols (cf., [18, 15]). Namely, we start with a configuration in which validity assures the common output is 0, and, while maintaining the same output, we gradually adjust it into a configuration in which validity assures the common output is 1, thus obtaining a contradiction. For randomized protocols, the challenge is to maintain the invariant of the output, even when the probability of halting is far from 1. We make the following observations:

$$\text{Supermajority execution:} \quad \operatorname{dist}(\boldsymbol{v}, b^n) \le t \implies \Pi(\boldsymbol{v}) = b. \tag{1}$$

That is, in an honest execution of Π, if there is a supermajority ($\ge n - t$) of b's in the input vector, then the parties output b with probability 1. Equation (1) follows by agreement and validity by considering an adversary corrupting exactly those parties with input $v_i \neq b$, and otherwise not deviating from the protocol.

$$\text{Neighboring executions (N1):} \quad \operatorname{dist}(\boldsymbol{v}_0, \boldsymbol{v}_1) \le t \implies \Pr_{\boldsymbol{r}}\left[\Pi(\boldsymbol{v}_0; \boldsymbol{r}) = \Pi(\boldsymbol{v}_1; \boldsymbol{r})\right] \ge \gamma. \tag{2}$$

That is, for two input vectors that are at most t-far (i.e., the resiliency threshold), the probability that the executions on these vectors yield the same output when using the same randomness is bounded below by the halting probability. To see why Equation (2) holds, consider the following adversary corrupting subset $\mathcal{C}$, for $\mathcal{C}$ being the set of indices where $\boldsymbol{v}$ and $\boldsymbol{v}'$ disagree. For an arbitrary partition $\{\overline{\mathcal{C}}_0, \overline{\mathcal{C}}_1\}$ of $\overline{\mathcal{C}}$, the adversary instructs $\mathcal{C}$ to send messages according to $\boldsymbol{v}_0$ to $\overline{\mathcal{C}}_0$ and according to $\boldsymbol{v}_1$ to $\overline{\mathcal{C}}_1$, respectively. With probability at least γ, all parties halt at the first round, and, by perfect agreement, all parties compute the same output.[7] Since parties in $\overline{\mathcal{C}}_b$ cannot

[7] In the above, we have chosen to ignore a crucial subtlety. In an execution of the protocol, it may be the case that there is a suitable message (according to $\boldsymbol{v}_0$ or $\boldsymbol{v}_1$) to prevent halting, yet the adversary cannot determine which one to send. In further sections, we address this issue by taking a random partition of $\overline{\mathcal{C}}$ (rather than an arbitrary one). By doing so, we introduce an error-term of $1/2^{n-t}$ when we upper bound the halting probability γ.

distinguish this execution from a halting execution of $\Pi(\boldsymbol{v}_b; \boldsymbol{r})$, Equation (2) follows.

We deduce that if there are more than $n/3$ corrupt parties, then the halting probability is 0; this follows by combining the two observations above for $\boldsymbol{v}_0 = 0^{n-t}1^t$ and $\boldsymbol{v}_1 = 0^t 1^{n-t}$. Namely, by Equation (1), it holds that $\Pr_{\boldsymbol{r}}[\Pi(\boldsymbol{v}_0; \boldsymbol{r}) = \Pi(\boldsymbol{v}_1; \boldsymbol{r})] = 0$. Thus, by Equation (2), $\gamma = 0$.

2.2 Second-Round Halting – Arbitrary Protocols

In this subsection we explain our bound for second-round halting of arbitrary protocols. Assume the honest parties of Π halt at the end of the second round with probability $\gamma > 0$ when facing t corruptions (on every input). Let $t = (1/3 + \varepsilon)n$, for $\varepsilon > 0$. In spirit, the attack follows the footsteps of the single-round case described above. We show that neighboring executions compute the same output with good enough probability (related to the halting probability), and lower-bound the latter using the supermajority observation. There is, however, a crucial difference between the first-round and second-round cases; the honest parties can use the second round to detect whether (some) parties are sending inconsistent messages. Thus, the second round of the protocol can be used to "catch-and-discard" parties that are pretending to have different inputs to different parties, and so our previous attack breaks down (In the one-round case, we exploit the fact that the honest parties cannot verify the consistency of the messages they received.). Still, we show that there is a different attack that violates the agreement of any "too-good" scheme.

At a very high level, the idea for proving the neighboring property is to *gradually* increase the set of honest parties towards which the adversary behaves according to $\boldsymbol{v}_1$ (for the remainder it behaves according to $\boldsymbol{v}_0$, which is a decreasing set of parties). While the honest parties might identify the attacking parties and discard their messages, they should still agree on the output and halt at the conclusion of the second round with high probability. We exploit this fact to show that at the two extremes (where the adversary is merely playing honestly according to $\boldsymbol{v}_0$ and $\boldsymbol{v}_1$, respectively), the honest parties behave essentially the same. Therefore, if at one extreme (for $\boldsymbol{v}_0$) the honest parties output b, it follows that they also output b at the other extreme (for $\boldsymbol{v}_1$), which proves the neighboring property for the second-round case.

We implement the above by augmenting the one-round attack as follows. In addition to corrupting a set of parties that feign different inputs to different parties, the adversary corrupts an extra set of parties that is inconsistent with regards to the messages it received from the first set of corrupted parties. To distinguish between the two sets of corrupted parties, the former (first) will be referred to as "pivot" parties (since they pivot their input) and will be denoted $\mathcal{P}$, and the latter will be referred to as "propagating" parties (since they carefully choose what message to propagate at the second round) and will be denoted $\mathcal{L}$. We emphasize that the propagating parties deviate from the protocol only at the second round and only with regards to the messages received by the pivot parties (not with regards to their input – as is the case for the pivot parties). In more detail, we partition $\overline{\mathcal{P}} = [n] \setminus \mathcal{P}$ into $\ell = \lceil 1/\varepsilon \rceil$ sets $\{\mathcal{L}_1, \ldots, \mathcal{L}_\ell\}$, and we show that, unless there exists i such that parties in $\mathcal{C} = \mathcal{P} \cup \mathcal{L}_i$ violate agreement (explained below), the following must hold for neighboring executions.

$$\begin{aligned}&\text{Neighbouring executions (N2):} \quad \operatorname{dist}(\boldsymbol{v}_0, \boldsymbol{v}_1) \leq n/3 \implies \\ &\Pr[\Pi(\boldsymbol{v}_0) = b \text{ in two rounds}] \geq \Pr[\Pi(\boldsymbol{v}_1) = b \text{ in two rounds}] - 2(\ell+1)^2 \cdot (1-\gamma).\end{aligned} \tag{3}$$

That is, for two input vectors that are at most $n/3$–far, the difference in probability that two distinct executions (for each input vector) yield the same output within two rounds is roughly upper-bounded by the quantity $(1-\gamma)/\varepsilon^2$ (i.e., non-halting probability divided by ε^2). To see that Equation (3) holds true, fix $\boldsymbol{v}_0, \boldsymbol{v}_1 \in \{0,1\}^n$ of hamming distance at most $n/3$, and let $\mathcal{P}$ be the set of indices where $\boldsymbol{v}_0$ and $\boldsymbol{v}_1$ differ. Consider the following $\ell+1$ distinct variants of Π, denoted $\{\Pi_0, \ldots, \Pi_\ell\}$; in protocol Π_i, parties in $\mathcal{P}$ send messages to $\mathcal{L}_1, \ldots, \mathcal{L}_i$ according to the input prescribed by $\boldsymbol{v}_1$ and to $\mathcal{L}_{i+1}, \ldots, \mathcal{L}_\ell$ according to the input prescribed by $\boldsymbol{v}_0$, respectively. All other parties follow the instructions of Π for input $\boldsymbol{v}_0$. We write $\Pi_i = b$ to denote the event that the parties not in $\mathcal{P}$ output b. Notice that the endpoint executions Π_0 and Π_ℓ are identical to honest executions with input $\boldsymbol{v}_0$ and $\boldsymbol{v}_1$, respectively. Let Halt_i denote the event that the parties not in $\mathcal{P}$ halt at the second round in an execution of Π_i. We point out that $\Pr[\neg\mathsf{Halt}_i] \leq (\ell+1)\cdot(1-\gamma)$, since otherwise the adversary corrupting $\mathcal{P}$ and running Π_i, for a random $i \in (\ell) = \{0, \ldots, \ell\}$, prevents halting with probability greater than $1-\gamma$. Next, we inductively show that

$$\Pr[\Pi_i = b \wedge \mathsf{Halt}_i] \geq \Pr[\Pi_0 = b \wedge \mathsf{Halt}_0] - 2i \cdot (\ell+1)\cdot(1-\gamma), \tag{4}$$

for every $i \in (\ell)$, which yields the desired expression for $i = \ell$. In pursuit of contradiction, assume Equation (4) does not hold, and let i denote the smallest index for which it does not hold (observe that $i \neq 0$, by definition). Notice that

$$\begin{aligned}
&\Pr[(\Pi_{i-1} = b \wedge \mathsf{Halt}_{i-1}) \wedge (\Pi_i \neq b \wedge \mathsf{Halt}_i)] \\
&\qquad \geq \Pr[\Pi_{i-1} = b \wedge \mathsf{Halt}_{i-1}] - \Pr[\Pi_i = b \vee \neg\mathsf{Halt}_i] \\
&\qquad \geq \Pr[\Pi_{i-1} = b \wedge \mathsf{Halt}_{i-1}] - \Pr[\Pi_i = b \wedge \mathsf{Halt}_i] - \Pr[\neg\mathsf{Halt}_i] \\
&\qquad > 2\cdot(\ell+1)\cdot(1-\gamma) - \Pr[\neg\mathsf{Halt}_i] \\
&\qquad = (\ell+1)\cdot(1-\gamma) \geq 0.
\end{aligned}$$

It follows that an adversary corrupting $\mathcal{C} = \mathcal{P} \cup \mathcal{L}_i$ causes disagreement with non-zero probability by acting as follows: parties in $\mathcal{P}$ and $\mathcal{L}_i$ send messages according to Π_i and Π_{i-1} to $\overline{\mathcal{C}}_0$ and $\overline{\mathcal{C}}_1$, respectively, where $\{\overline{\mathcal{C}}_0, \overline{\mathcal{C}}_1\}$ is an arbitrary partition of $\overline{\mathcal{C}} = [n] \setminus \mathcal{P} \cup \mathcal{L}_i$. Since disagreement is ruled out by assumption, we deduce Equations (3) and (4). To conclude, we combine the supermajority property (Equation (1)) with the neighboring property (Equation (3)) with $(\boldsymbol{v}_0, \boldsymbol{v}_1) = (0^{n-t}1^t, 0^t1^{n-t})$ and $b = 1$. Namely, $\Pr[\Pi(\boldsymbol{v}_0) = 1 \text{ in two rounds}] = 0$, by supermajority, and $\Pr[\Pi(\boldsymbol{v}_1) = 1^n \text{ in two rounds}] \geq \gamma$, by supermajority and halting. It follows that $0 \geq \gamma - 2(\ell+1)^2\cdot(1-\gamma)$, by Equation (3), and thus $1 - \frac{1}{2(\ell+1)^2+1} \geq \gamma$, which yields the desired expression.

2.3 Second-Round Halting – Public-Randomness Protocols

In Section 2.2, we ruled out "very good" second-round halting for arbitrary protocols via an efficient locally consistent attack. Recall that if the halting probability is too good (probability almost one), then there is a somewhat simple attack that violates agreement and/or validity. In this subsection, we discuss ruling out *any* second-round halting, i.e., halting probability bounded away from zero, for public-randomness protocols.

We first explain why the attack – as is – does not rule out second-round halting. Assume that at the first round, the parties of Π send a deterministic function of their input, and at the second round they send the messages they received at the first round together with a uniform random bit. On input $\boldsymbol{v}$ and randomness $\boldsymbol{r}$, the parties are instructed *not* to halt at the second round, if a supermajority ($\geq n-t$) of the v_i's are in agreement and $\mathrm{maj}(r_1, \ldots, r_n) \neq \mathrm{maj}(v_1, \ldots, v_n)$, i.e., the majority of the random bits does not agree with the supermajority of the inputs. In all other cases, the parties are instructed to output $\mathrm{maj}(r_1, \ldots, r_n)$. It is not hard to see that this protocol will halt with probability 1/2, even in the presence of the previous locally consistent adversary (regardless of the choice of propagating parties $\mathcal{L}_i$). More generally, if the randomness uniquely determines the output, the protocol designer can ensure that halting does not result in disagreement, by partitioning the randomness appropriately, and thus foiling the previous attack.[8]

To overcome the above apparent obstacle, we introduce another dimension to our locally consistent attack; we instruct an extra set of corrupted parties to abort at the second round without sending their second-round messages. By utilizing aborting parties, the adversary can potentially decouple the output/halting from the parties' randomness and thus either prevent halting or cause disagreement. We explain below how to rule out second-round halting for a rather unrealistic class of public-randomness protocol. What makes the class of protocols unrealistic is that we assume security holds against unbounded locally consistent adversaries, and the protocol prescribes only a single bit of randomness per party per round. That being said, this case illustrates nicely our attack, and it also makes an interesting connection to Boolean functions analysis (namely, the KKL theorem [27]). For general public-randomness protocols, we only know how to analyze the aforementioned attack assuming Conjecture 1.5.

"Superb" Single-Coin Protocols. A BA protocol Π is t-*superb* if agreement and validity hold perfectly against an adaptive *unbounded* locally consistent adversary corrupting at most t parties, i.e., the probability that such an adversary violates agreement or validity is 0. A public-randomness protocol is *single-coin*, if, at any given round, each party samples a single unbiased bit.

Theorem 2.1 (Second-round halting, superb single-coin protocols)**.** *For every $\varepsilon > 0$ there exists $c > 0$ such that the following holds for large enough n. For $t = (1/3+\varepsilon)n$, let Π be a t-superb, single-coin, n-party public-randomness Byzantine agreement protocol and let γ denote the probability that the protocol halts in the second round under a locally consistent attack. Then, $\gamma \leq n^{-c}$.*

We assume for simplicity that the parties do not sample any randomness at the first round, and write $\boldsymbol{r} \in \{0,1\}^n$ for the vector of bits sampled by the parties at the second round, i.e., $\boldsymbol{r}_i$ is a uniform random bit sampled by P_i.

As discussed above, out attack uses an additional set of corrupted parties of size $\sigma \cdot n$, dubbed the "aborting" parties and denoted $\mathcal{S}$, that abort indiscriminately at the second round (the value of σ is set to $\lfloor \varepsilon/4 \rfloor$ and $\ell = 2 \cdot \lceil 1/\varepsilon \rceil$ to accommodate for the new set of corrupted parties, i.e., $|\mathcal{L}_i| \leq n \cdot \varepsilon/2$). In more detail, analogously to the previous analysis, we consider $(\ell+1) \cdot \binom{n}{\sigma n}$ distinct variants of Π, denoted $\{\Pi_i^{\mathcal{S}}\}_{i,\mathcal{S}}$ and indexed by $i \in (\ell)$ and $\mathcal{S} \subseteq [n]$ of size σn, as follows. In protocol $\Pi_i^{\mathcal{S}}$, parties in $\mathcal{P}$ send messages to $\mathcal{L}_1, \ldots, \mathcal{L}_i$ according to the input prescribed by $\boldsymbol{v}_1$, and to $\mathcal{L}_{i+1}, \ldots, \mathcal{L}_\ell$ according to the input prescribed by $\boldsymbol{v}_0$ (recall that $\mathcal{P}$ is exactly those indices where $\boldsymbol{v}_0$ and $\boldsymbol{v}_1$ differ). Parties in $\mathcal{S}$ act according to $\mathcal{P}$ or $\mathcal{L}_j$, for the relevant j, except that they abort at the second round without sending their second round messages. We write $\Pi_i^{\mathcal{S}}(\boldsymbol{r}) = b$ to denote the event that the parties not in $\mathcal{P} \cup \mathcal{S}$ output b, where the parties' second-round randomness is equal to $\boldsymbol{r}$. Let $\mathsf{Halt}_i^{\mathcal{S}}$ denote the event that all parties not in $\mathcal{P} \cup \mathcal{S}$ halt at the second round in an execution of $\Pi_i^{\mathcal{S}}$, and define $\mathcal{R}_i^{\mathcal{S}}(b) = \{\boldsymbol{r} \in \{0,1\}^n \text{ s.t. } \Pi_i^{\mathcal{S}}(\boldsymbol{r}) = b \wedge \mathsf{Halt}_i^{\mathcal{S}}\}$. The following holds:

$$\text{Neighbouring executions (N2}\dagger\text{):} \qquad (5)$$
$$\forall \boldsymbol{v}_0, \boldsymbol{v}_1 \in \{0,1\}^n \text{ with } \operatorname{dist}(\boldsymbol{v}_0, \boldsymbol{v}_1) \leq t - \varepsilon n, \quad \forall b \in \{0,1\}, i \in [\ell] = \{1, \ldots, \ell\}:$$
$$\left(\forall \mathcal{S}\colon \Pr\left[\Pi_{i-1}^{\mathcal{S}} = b \wedge \mathsf{Halt}_{i-1}^{\mathcal{S}}\right] \geq \gamma/2\right) \implies \left(\forall \mathcal{S}\colon \Pr\left[\Pi_i^{\mathcal{S}} = b \wedge \mathsf{Halt}_i^{\mathcal{S}}\right] \geq \gamma/2\right).$$

[8] In Section 2.2, halting was close to 1 and thus the randomness was necessarily ambiguous regarding the output.

In words, for both $b \in \{0,1\}$: if $\Pi_{i-1}^{\mathcal{S}} = b$ and halts in two rounds with large probability ($\geq \gamma/2$), for every $\mathcal{S}$, then $\Pi_i^{\mathcal{S}} = b$ and halts in two rounds with large probability, for every $\mathcal{S}$. Before proving Equation (5), we show how to use it to derive Theorem 2.1. We apply Equation (5) for $(\boldsymbol{v}_0, \boldsymbol{v}_1) = (0^{n-t}1^t, 0^t1^{n-t})$, $b = 0$ and $i = \ell$, in combination with the properties of validity and supermajority, Equation (1). Namely, by validity and supermajority, a random execution of Π on input $\boldsymbol{v}_0$ where the parties in $\mathcal{S}$ abort at the second round yields output 0 with probability at least $\gamma/2$, for every $\mathcal{S} \in \binom{[n]}{\sigma n}$. Therefore, applying Equation (5) for $(\boldsymbol{v}_0, \boldsymbol{v}_1) = (0^{n-t}1^t, 0^t1^{n-t})$, $b = 0$ and $i = \ell$, we deduce that a random execution of Π on input $\boldsymbol{v}_1$ where the parties in $\mathcal{S}$ abort at the second round yields output 0 with probability at least $\gamma/2$, for every $\mathcal{S} \in \binom{[n]}{\sigma n}$. The latter violates either supermajority or validity – contradiction. We conclude the proof of Theorem 2.1 by proving Equation (5). We prove Equation (5) using the following corollary of the seminal KKL theorem [27] from Bourgain et al. [7]. (Recall that $\mathcal{R}|_{\overline{\mathcal{S}}}$ is the projection of $\mathcal{R}$ on the index-set $\overline{\mathcal{S}}$.)

Lemma 2.2. *For every $\sigma, \delta \in (0,1)$, there exists $c > 0$ s.t. the following holds for large enough n. Let $\mathcal{R} \subseteq \{0,1\}^n$ be s.t. $|\mathcal{R}|_{\overline{\mathcal{S}}}| \leq (1-\delta) \cdot 2^{(1-\sigma)n}$, for every $\mathcal{S} \subseteq [n]$ of size σn. Then, $|\mathcal{R}| \leq n^{-c} \cdot 2^n$.*

Loosely speaking, Lemma 2.2 states that for a set $\mathcal{R} \subseteq \{0,1\}^n$, if the size of every projection on a constant fraction of indices is bounded away from one (in relative size), then the size of $\mathcal{R}$ is vanishingly small (again, in relative size).

Going back to the proof, suppose Equation (5) does not hold for $b = 0$, i.e., there exists $\mathcal{S}$ such that $|\mathcal{R}_i^{\mathcal{S}}(0)| < \gamma/2 \cdot 2^n$, and $|\mathcal{R}_{i-1}^{\mathcal{S}'}(0)| \geq \gamma/2 \cdot 2^n$, for every relevant $\mathcal{S}'$. We prove Equation (5) by proving Equations (6) and (7), which result in contradiction via Lemma 2.2.

$$\text{Halting:} \qquad |\mathcal{R}_i^{\mathcal{S}}(1)| \geq \gamma/2 \cdot 2^n \tag{6}$$

$$\text{Perfect agreement:} \qquad \forall \mathcal{S}': \quad |\mathcal{R}_i^{\mathcal{S}}(1)|_{\overline{\mathcal{S}'}}| \leq (1-\gamma/2) \cdot 2^{(1-\sigma)n} \tag{7}$$

Equation (6) follows by the halting property of $\Pi_i^{\mathcal{S}}$, since the execution halts if and only if $\boldsymbol{r} \in \mathcal{R}_i^{\mathcal{S}}(1) \cup \mathcal{R}_i^{\mathcal{S}}(0)$, and, by assumption, $|\mathcal{R}_i^{\mathcal{S}}(0)| < \gamma/2 \cdot 2^n$. Equation (7) follows from $|\mathcal{R}_{i-1}^{\mathcal{S}'}(0)| \geq \gamma/2 \cdot 2^n$ (by assumption), and $\mathcal{R}_i^{\mathcal{S}}(1)|_{\overline{\mathcal{S}'}} \cap \mathcal{R}_{i-1}^{\mathcal{S}'}(0)|_{\overline{\mathcal{S}'}} = \emptyset$, for every $\mathcal{S}'$. The latter holds since $\boldsymbol{r}|_{\overline{\mathcal{S}'}} = \boldsymbol{r}'|_{\overline{\mathcal{S}'}}$ and $\boldsymbol{r}' \in \mathcal{R}_{i-1}^{\mathcal{S}'}(0)$ implies $\boldsymbol{r} \in \mathcal{R}_{i-1}^{\mathcal{S}'}(0)$, and by considering the attacker controlling $\mathcal{P}$, $\mathcal{L}_i$, $\mathcal{S}$ and $\mathcal{S}'$ and sending messages according to $\Pi_i^{\mathcal{S}}$ and $\Pi_{i-1}^{\mathcal{S}'}$ to $\overline{\mathcal{C}}_0$ and $\overline{\mathcal{C}}_1$, respectively, where $\{\overline{\mathcal{C}}_0, \overline{\mathcal{C}}_1\}$ is an arbitrary partition of $\overline{\mathcal{C}} = [n] \setminus \mathcal{P} \cup \mathcal{L}_i \cup \mathcal{S} \cup \mathcal{S}'$.

Remark 2.3. *For superb, single-coin, public-randomness protocol, repeated application of Equation (2) and Lemma 2.2 rules out second-round halting for arbitrary (constant) fraction of corrupted parties (and not only $n/3$ fraction).*

General (Public-Randomness) Protocols. The analysis above crucially relies on the superb properties of the protocol. While it can be generalized for protocols with near-perfect statistical security and constant-bit randomness, we only manage to analyze the most general case (i.e., protocols with non-perfect computational security and arbitrary-size randomness) assuming Conjecture 1.5. Very roughly (and somewhat inaccurately), when applying the above attack on general public-randomness protocols, the following happens for some $\delta > 0$ and both values of $b \in \{0,1\}$: for $(1-\delta)$-fraction of possible aborting subsets $\mathcal{S}$, the probability that the honest parties halt in two rounds and output the same value b, whether parties in $\mathcal{S}$ all abort or not, is at least λ (i.e., the halting probability). Assuming Conjecture 1.5, the above yields that with probability δ over the randomness and $\mathcal{S}$, the honest parties under the attack output opposite values depending whether the parties in $\mathcal{S}$ abort or not. It thus follows that the agreement of the protocol is at most δ. We refer the reader to Appendix D.2 for the full details.

Bibliography

[1] I. Abraham, T. H. Chan, D. Dolev, K. Nayak, R. Pass, L. Ren, and E. Shi. Communication complexity of Byzantine agreement, revisited. PODC 2019 (to appear), 2019.

[2] I. Abraham, S. Devadas, D. Dolev, K. Nayak, and L. Ren. Synchronous Byzantine agreement with expected O(1) rounds, expected o(n^2) communication, and optimal resilience. In *Financial Cryptography and Data Security*, 2019.

[3] H. Attiya and K. Censor-Hillel. Lower bounds for randomized consensus under a weak adversary. *SIAM Journal on Computing*, 39(8):3885–3904, 2010.

[4] M. Ben-Or. Another advantage of free choice: Completely asynchronous agreement protocols (extended abstract). In *Proceedings of the 2nd Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 27–30, 1983.

[5] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1–10, 1988.

[6] E. Ben-Sasson, A. Chiesa, M. Green, E. Tromer, and M. Virza. Secure sampling of public parameters for succinct zero knowledge proofs. In *IEEE Symposium on Security and Privacy*, pages 287–304, 2015.

[7] J. Bourgain, J. Kahn, and G. Kalai. Influential coalitions for Boolean functions. https://arxiv.org/abs/1409.3033, 2014.

[8] S. Bowe, A. Gabizon, and M. D. Green. A multi-party protocol for constructing the public parameters of the pinocchio zk-snark. In *Financial Cryptography and Data Security FC*, pages 64–77, 2018.

[9] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In *Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 173–186, 1999.

[10] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–19, 1988.

[11] J. Chen and S. Micali. Algorand. In *CoRR*, 2016. http://arxiv.org/abs/1607.01341.

[12] B. Chor, M. Merritt, and D. B. Shmoys. Simple constant-time consensus protocols in realistic failure models. *Journal of the ACM*, 36(3):591–614, 1989.

[13] R. Cohen, S. Coretti, J. A. Garay, and V. Zikas. Probabilistic termination and composability of cryptographic protocols. In *Advances in Cryptology – CRYPTO 2016, part III*, pages 240–269, 2016.

[14] R. Cohen, S. Coretti, J. Garay, and V. Zikas. Round-preserving parallel composition of probabilistic-termination cryptographic protocols. In *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 37:1–37:15, 2017.

[15] D. Dolev and R. Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983.

[16] D. Dolev, R. Reischuk, and H. R. Strong. Early stopping in Byzantine agreement. *Journal of the ACM*, 37(4):720–741, 1990.

[17] P. Feldman and S. Micali. An optimal probabilistic protocol for synchronous Byzantine agreement. *SIAM Journal on Computing*, 26(4):873–933, 1997.

[18] M. J. Fischer and N. A. Lynch. A lower bound for the time to assure interactive consistency. *Information Processing Letters*, 14(4):183–186, 1982.

[19] M. J. Fischer, N. A. Lynch, and M. Merritt. Easy impossibility proofs for distributed consensus problems. In *Proceedings of the 23th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 59–70, 1985.

[20] M. Fitzi and J. A. Garay. Efficient player-optimal protocols for strong and differential consensus. In *Proceedings of the 22th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 211–220, 2003.

[21] E. Friedgut. Boolean functions with low average sensitivity depend on few coordinates. *Combinatorica*, 18(1):27–35, 1998.

[22] J. A. Garay and Y. Moses. Fully polynomial Byzantine agreement in t+1 rounds. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing (STOC)*, pages 31–41, 1993.

[23] J. A. Garay, J. Katz, C. Koo, and R. Ostrovsky. Round complexity of authenticated broadcast with a dishonest majority. In *Proceedings of the 48th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 658–668, 2007.

[24] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand: Scaling Byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles (SOSP)*, pages 51–68, 2017.

[25] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC)*, pages 218–229, 1987.

[26] S. Goldwasser, Y. T. Kalai, and S. Park. Adaptively secure coin-flipping, revisited. In *Proceedings of the 42th International Colloquium on Automata, Languages, and Programming (ICALP), part II*, pages 663–674, 2015.

[27] J. Kahn, G. Kalai, and N. Linial. The influence of variables on Boolean functions (extended abstract). In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 68–80, 1988.

[28] A. R. Karlin and A. C. Yao. Probabilistic lower bounds for Byzantine agreement and clock synchronization. Unpublished manuscript, 1986.

[29] J. Katz and C. Koo. On expected constant-round protocols for Byzantine agreement. In *Advances in Cryptology – CRYPTO 2006*, pages 445–462, 2006.

[30] J. Kubiatowicz, D. Bindel, Y. Chen, S. E. Czerwinski, P. R. Eaton, D. Geels, R. Gummadi, S. C. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Y. Zhao. Oceanstore: An architecture for global-scale persistent storage. In *ASPLOS-IX Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 190–201, 2000.

[31] L. Lamport, R. E. Shostak, and M. C. Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[32] Y. Lindell, A. Lysyanskaya, and T. Rabin. On the composition of authenticated Byzantine agreement. *Journal of the ACM*, 53(6):881–917, 2006.

[33] S. Micali. Very simple and efficient Byzantine agreement. In *Proceedings of the 8th Annual Innovations in Theoretical Computer Science (ITCS) conference*, pages 6:1–6:1, 2017.

[34] S. Micali and V. Vaikuntanathan. Optimal and player-replaceable consensus with an honest majority. Unpublished manuscript, 2017.

[35] E. Mossel, R. O'Donnell, O. Regev, J. E. Steif, and B. Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, Dec 2006. ISSN 1565-8511.

[36] E. Mossel, K. Oleszkiewicz, and A. Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, Jun 2013. ISSN 1420-8970.

[37] R. O'Donnell. *Analysis of Boolean Functions.* Cambridge University Press, 2014. doi: 10.1017/CBO9781139814782.

[38] R. Pass and E. Shi. Hybrid consensus: Efficient consensus in the permissionless model. In *Proceedings of the 31st International Symposium on Distributed Computing (DISC)*, pages 39:1–39:16, 2017.

[39] R. Pass and E. Shi. Thunderella: Blockchains with optimistic instant confirmation. In *Advances in Cryptology – EUROCRYPT 2018, part II*, pages 3–33, 2018.

[40] M. C. Pease, R. E. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27(2):228–234, 1980.

[41] B. Pfitzmann and M. Waidner. Unconditional Byzantine agreement for any number of faulty processors. In *Proceedings of the 9th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 339–350, 1992.

[42] M. O. Rabin. Randomized Byzantine generals. In *Proceedings of the 24th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 403–409, 1983.

[43] R. Turpin and B. A. Coan. Extending binary Byzantine agreement to multivalued Byzantine agreement. *Information Processing Letters*, 18(2):73–76, 1984.

[44] A. C. Yao. Protocols for secure computations (extended abstract). In *Proceedings of the 23th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 160–164, 1982.

A Introduction (Cont'd)

A.1 Locally Consistent Security to Malicious Security

As briefly mentioned in Section 1.1, protocols that are secure against locally consistent adversaries can be compiled to tolerate arbitrary malicious adversaries. We now elaborate on this transformation. The compiler requires a PKI for signatures and VRF. Every party P_i computes the messages for round r using the random coins obtained by evaluating the VRF over (i, r). Next, P_i signs and sends the messages, and proves to each receiver in zero knowledge that (1) it acted consistently with some input bit, the random coins computed by the VRF, and correctly signed incoming messages from some of the parties, and (2) that all prior messages sent by P_i are consistent with respect to the same input bit, random coins, and incoming messages from previous rounds.

When a public-randomness protocol can be executed over authenticated yet non-private channels, the compilation presented above can be made much more efficient. Instead of proving in zero knowledge the consistency of each message, each party concatenates to each message all of its incoming messages from the previous round. A receiver can now locally verify the coins are proper (as assured by the VRF), that the incoming messages are properly signed, and that the message is correctly generated from the internal state of the sender.

Theorem A.1 (Locally consistent to malicious security, folklore, informal)**.** *Assume PKI for digital signatures and VRF, then a BA protocol secure against locally consistent adversaries, can be compiled into a maliciously secure BA protocol with the same parameters, apart from a constant blowup in the round complexity (no blowup for public-randomness protocols).*

A.2 Additional Related Work

Following the work of Feldman and Micali [17] in the two-thirds majority setting, Katz and Koo [29] improved the expected round complexity to 23, and Micali [33] to 9. In the honest-majority setting, Fitzi and Garay [20] showed expected-constant-round protocol and Katz and Koo [29] expected 56 rounds. Micali and Vaikuntanathan [34] adjusted the technique from [33] to the honest majority case. Abraham et al. [2] achieved expected 10 rounds assuming static corruptions and expected 16 rounds assuming adaptive corruptions. Abraham et al. [1] constructed an expected-constant-round protocol tolerating $(1/2 - \epsilon)n$ adaptive corruptions with sublinear communication complexity. In the dishonest-majority setting, Garay et al. [23] constructed a broadcast protocol with expected $O(k)$ rounds, tolerating $t < n/2 + k$ corruptions.

Attiya and Censor-Hillel [3] extended the results of Chor et al. [12] and of Karlin and Yao [28] on guaranteed termination of randomized BA protocols to the asynchronous setting, and provided a tight lower bound.

Randomized protocols with expected constant round complexity have *probabilistic termination*, which requires delicate care with respect to composition (i.e., their usage as subroutines by higher-level protocols). Parallel composition of randomized BA protocols was analyzed in [4, 20], sequential composition in [32], and universal composition in [13, 14].

B Our Lower Bounds

In this section, we formally state our lower bounds on the round complexity of Byzantine agreement protocols. The communication and adversarial models as well as the notion of Byzantine agreement protocols we consider are given in Appendix B.1, and our bounds are formally stated in Appendix B.2.

B.1 The Model

B.1.1 Protocols

All protocols considered in this paper are PPT (probabilistic polynomial time): the running time of every party is polynomial in the (common) security parameter (given as a unary string). We only consider boolean-input boolean-output protocols: apart from the common security parameter, all parties have a single input bit, and each of the honest parties outputs a single bit. For an n-party protocol Π, an input vector $\boldsymbol{v} \in \{0,1\}^n$ and randomness $\boldsymbol{r}$, let $\Pi(\boldsymbol{v};\boldsymbol{r})$ denote the output vector of the parties in an (honest) execution with party P_i's input being $\boldsymbol{v}_i$ and randomness $\boldsymbol{r}_i$. For a set of parties $\mathcal{P} \subseteq [n]$, we denote by $\Pi(\boldsymbol{v};\boldsymbol{r})_{\mathcal{P}}$ the output vector of the parties in $\mathcal{P}$.

The protocols we consider might have a *setup phase* in which before interaction starts a trusted party distributes (correlated) values between the parties. We only require the security to hold for a *single* use of the setup parameters (in reality, these parameters are set once and then used for many interactions). This, however, only makes our lower bound stronger.

The communication model is *synchronous*, meaning that the protocols proceed in rounds. In each round every party can send a message to every other party over a private and authenticated channel. (Allowing the protocol to be executed over private channels makes our lower bounds stronger.) It is guaranteed that all of the messages that are sent in a round will arrive at their destinations by the end of that round.

B.1.2 Adversarial Model

We focus on *rushing adversaries*. Adversaries that can base their current round on the messages sent to him (by the honest parties) in the same round.

We consider both adaptive and non-adaptive (also known as, static) adversaries. An adaptive adversary can choose which parties to corrupt for the next round immediately after the conclusion of the previous round but before seeing the next round's messages. If a party has been corrupted then it is considered corrupt for the rest of the execution. A non-adaptive (static) adversary chooses which parties to corrupt *before* the execution of the protocol begins (i.e., before the setup phase, if such exists). We measure the success probability of the latter adversaries as the expectation over their choice of corrupted parties.

Locally consistent adversaries. As discussed in Section 1.1, our attack requires very limited capabilities from each corrupted party: to prematurely abort, and to lie about its input bit and incoming messages from other corrupted parties. In particular, a corrupted party tosses its local coins honestly and does not lie about incoming messages from honest parties. We now present the formal definition.

Definition B.1 (locally consistent adversaries)**.** *Let $\Pi = (\mathsf{P}_1, \ldots, \mathsf{P}_n)$ be an n-party protocol and let $\{\alpha^j_{i,i'}\}_{i,i' \in [n], j \in \mathbb{N}}$ be its set of next-message functions, i.e.,*

$$m^j_{i,i'} = \alpha^j_{i,i'}(b; r; (m^1_{1,i}, \ldots, m^1_{n,i}), \ldots, (m^{j-1}_{1,i}, \ldots, m^{j-1}_{n,i}))$$

is the message party P_i *sends to party* $\mathsf{P}_{i'}$ *in the* j*'th round, given that its input bit is* b*, the random coins it flipped till now are* r*, and in round* $j' < j$*, it got the message* $m^{j'}_{i'',i}$ *from party* $\mathsf{P}_{i''}$*. An adversary taking the role of* P_i *is said to be* locally consistent *with respect to* Π*, if it* flips its random coins honestly*, and the message it sends in the* j*'th round to party* $\mathsf{P}_{i'}$ *takes one of the following two forms:*

Abort: *the message* $\perp$*.*

Input and message selection: *a set of messages* $\{m_\ell\}_{\ell=1}^{k}$ *such that for each* $\ell \in [k]$*:*

$$m_\ell = \alpha^{j}_{i,i'}(b_\ell; r; ((m^1_1)_1, \ldots, (m^1_n)_1), \ldots, ((m^{j-1}_1)_\ell, \ldots, (m^{j-1}_n)_\ell)),$$

where $b_\ell \in \{0,1\}$*,* r *are the coins* P_i *tossed (honestly) until now, and* $(m^{j'}_{i''})_\ell$*, for each* $j' < j$ *and* $i'' \neq i$*, is one of the messages it received from party* $\mathsf{P}_{i''}$ *in the* j*'th round.*

That is, a locally consistent party P_i might send party $\mathsf{P}_{i'}$ a sequence of messages (and not one as instructed), each consistent with a possible choice of its input bit, and some of the messages it received in the previous round. In turn, this will enable party $\mathsf{P}_{i'}$, if corrupted, the freedom to choose in the next rounds the message of P_i it would like to act according to. Note that W.l.o.g, P_i will always sends a single message to the honest parties, as otherwise they will discard the messages.

A few remarks are in place.

1. While the above definition does not enforce between-rounds consistency (a party might send to another party a first round message consistent with input 0 and in the second round a message consistent with 1), compiling a given protocol so that every message party P_i sends to $\mathsf{P}_{i'}$ contains the previous messages P_i sent to $\mathsf{P}_{i'}$, will enforce such between-rounds consistency on locally consistent parties.

2. Using standard cryptographic techniques, a protocol secure against locally consistent adversaries can be compiled into one secure against arbitrary malicious adversaries, without hurting the efficiency and round complexity of the protocol "too much". If the protocol is *public randomness* (see Definition B.2) this reduction can be made extremely efficient, and in particular preserve the round complexity (see Appendix A.1.

3. The locally consistent parties considered in Appendices C and D do not take full advantage of the generality of Definition B.1. Rather, the parties considered either act honestly but abort at the conclusion of the first round, cheat in the first round and then abort, or cheat only in the second round and then abort.

B.1.3 Public-Randomness Protocols

In Section 1.1, we showed that the description of many natural protocols can be simplified when security is required to hold only against locally consistent adversaries. In this relaxed description a trusted setup phase and cryptographic assumptions are not required, and every party can publish the coins it locally tossed in each round.

Definition B.2 (Public-randomness protocols)**.** *A protocol has* public randomness*, if every party's message consists of two parts: the randomness it sampled in that round, and an arbitrary message which is a function of its view (input and coins tossed up to and including that point). The party's first message also contains its setup parameters, if such exist.*

B.1.4 Byzantine Agreement

We now formally define the notion of Byzantine agreement. Since we focus on lower bounds we will consider only the case of a single input bit and a single output bit. A more general notion of Byzantine agreement will include string input and string outputs. A generic reduction shows that the cost of agreeing on strings rather than bits is two additional rounds [43].

Definition B.3 (Byzantine Agreement)**.** *We associate the following properties with a* PPT *n-party Boolean input/output protocol Π.*

Agreement. *Protocol Π has (t, α)-*agreement*, if the following holds with respect to any* PPT *adversary controlling at most t parties in Π and any value of the non-corrupted parties' input bits: in a random execution of Π on sufficiently large security parameter, all non-corrupted parties output the* same *bit with probability at least $1 - \alpha$.*[9]

Validity. *Protocol Π has (t, β)-*validity*, if the following holds with respect to any* PPT *adversary controlling at most t parties in Π and an input bit b given as input to all non-corrupted parties: in a random execution of Π on sufficiently large security parameter, all non-corrupted parties output b with probability at least $1 - \beta$.*

Halting. *Protocol Π has (t, q, γ)-*halting*, if the following holds with respect to any* PPT *adversary controlling at most t parties in Π and any value of the non-corrupted parties' input bits: in a random execution of Π on sufficiently large security parameter, all non-corrupted parties halt within q rounds with probability at least γ.*

*Protocol Π is a $(t, \alpha, \beta, q, \gamma)$-*BA*, if it has (t, α)-*agreement*, (t, β)-*validity*, and (t, q, γ)-*halting*. If the protocol has a setup phase, then the above probabilities are taken with respect to this phase as well.*

Remark B.4 (Concrete security)**.** *Since we care about fixed values of a protocol's characteristics (i.e., agreement), the role of the security parameter in the above definition is to enable us to bound the running time of the parties and adversaries in consideration in a meaningful way, and to parametrize the cryptographic tools used by the parties (if there are any). Since the attacks we present are efficient assuming the protocol is efficient (in any reasonable sense), the bounds we present are applicable for a fixed protocol that might use a* fixed *cryptographic primitive, e.g., SHA-256.*

B.2 The Bounds

We proceed to present the formal statements of the three lower bounds.

First-round halting, arbitrary protocols. The first result bounds the halting probability of arbitrary protocols after a single round. Namely, for "small" values of α and β, the halting probability is "small" for $t \geq n/3$ and "close to 1/2" for $t \geq n/4$.

Theorem B.5 (restating Theorem 1.2)**.** *Let Π be a* PPT *n-party protocol that is $(t, \alpha, \beta, 1, \gamma)$-*BA *against first-round locally consistent, static, non-rushing adversaries. Then,*

[9] A more general definition would allow the parameter α (and the parameters β, γ below) to depend on the protocol's security parameter. But in this paper we focus on the case that α is a fixed value.

- $t \geq n/3$ *implies* $\gamma \leq 5\alpha + 2\beta + \mathsf{err}$.
- $t \geq n/4$ *implies* $\gamma \leq 1/2 + 5\alpha + \beta + \mathsf{err}$.

for $\mathsf{err} = 2^{t-n}$ *(*$\mathsf{err} = 0$ *for public-randomness protocols whose security holds against rushing adversaries).*

Second-round halting, arbitrary protocols. The second result bounds the halting probability of arbitrary protocols after two rounds.

Theorem B.6 (restating Theorem 1.3)**.** *Let* Π *be a* PPT *n-party protocol that is a* $(t, \alpha, \beta, 2, \gamma)$-$\mathsf{BA}$ *against locally consistent, static, non-rushing adversaries for* $t > n/4$*. Then* $\gamma \leq 1 + 2\alpha + \frac{\beta}{w^2} - \frac{1}{2w^2}$ *for* $w = \lceil (n - \lceil n/4 \rceil) / \lfloor t - n/4 \rfloor \rceil + 1$*.*

For $t = (1/4 + \varepsilon)n$ and "small" α, β the protocol might not halt at the conclusion of the second round with probability $\approx 1/\varepsilon^2$.

Second-round halting, public-randomness protocols. The third result bounds the halting probability of public-randomness protocols after two rounds. The result requires adaptive and rushing adversaries, and is based on Conjecture B.8 (stated in Appendix B.3 below).

Theorem B.7 (restating Theorem 1.4)**.** *Assume Conjecture B.8 holds. Then, for any* $\varepsilon_t, \varepsilon_\gamma > 0$ *there exists* $\alpha > 0$ *such that the following holds for large enough n: let* Π *be a* PPT *n-party, public-randomness protocol that is* $(t, \alpha, \beta = \varepsilon_\gamma^2/200, 2, \gamma)$-$\mathsf{BA}$ *against locally consistent, rushing, adaptive adversaries. Then,*

- $t \geq (1/3 + \varepsilon_t)n$ *implies* $\gamma < \varepsilon_\gamma$.
- $t \geq (1/4 + \varepsilon_t)n$ *implies* $\gamma < \frac{1}{2} + \varepsilon_\gamma$.

In particular, assuming the protocol has perfect agreement and validity, the protocol never halts in two rounds if the fraction of corrupted parties is greater than 1/3, and halts in two rounds with probability at most 1/2 if the fraction of corrupted parties is greater than 1/4.

The value of α in the theorem is (roughly) $\delta \cdot \varepsilon_t \cdot \varepsilon_\gamma^2$ where δ is the constant guaranteed by Conjecture B.8. We were not trying to optimize over the constants in the above statement, and in particular it seems that β can be pushed to ε_γ^2.

B.3 The Combinatorial Conjecture

Next, we provide the formal statement for the combinatorial conjecture used in Theorem B.7. For $n \in \mathbb{N}$ and $\sigma \in [0,1]$, let $\mathbf{D}_{n,\sigma}$ be the distribution induced on the subsets of $[n]$ by sampling each element independently with probability σ. For a finite alphabet Σ, a vector $\boldsymbol{x} \in \Sigma^n$, and a subset $\mathcal{S} \subseteq [n]$, define the vector $\perp_{\mathcal{S}}(\boldsymbol{x}) \in \Sigma^n$ by

$$\perp_{\mathcal{S}}(\boldsymbol{x})_i = \begin{cases} \perp, & i \in \mathcal{S}, \\ \boldsymbol{x}_i, & \text{otherwise.} \end{cases}$$

Conjecture B.8. *For any $\sigma, \lambda > 0$ there exists $\delta > 0$ such that the following holds for large enough $n \in \mathbb{N}$. Let Σ be a finite alphabet and let $\mathcal{A}_0, \mathcal{A}_1 \subseteq \{\Sigma \cup \perp\}^n$ be two sets such that for both $b \in \{0,1\}$:*

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} \left[\Pr_{\boldsymbol{r} \leftarrow \Sigma^n} \left[\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b \right] \geq \lambda \right] \geq 1 - \delta.$$

Then,

$$\Pr_{\substack{\boldsymbol{r} \leftarrow \Sigma^n \\ \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}} \left[\forall b \in \{0,1\}\colon \ \{\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b \neq \emptyset \right] \geq \delta.$$

C Lower Bounds on First-Round Halting

In this section, we present our lower bound for the probability of first-round halting in Byzantine agreement protocols.

Theorem C.1 (Bound on first-round halting. Theorem B.5 restated)**.** *Let Π be a* PPT *n-party protocol that is $(t, \alpha, \beta, 1, \gamma)$-$\mathsf{BA}$ against first-round locally consistent, static, non-rushing adversaries. Then,*

- *$t \geq n/3$ implies $\gamma \leq 5\alpha + 2\beta + \mathsf{err}$.*
- *$t \geq n/4$ implies $\gamma \leq 1/2 + 5\alpha + \beta + \mathsf{err}$.*

for $\mathsf{err} = 2^{t-n}$ ($\mathsf{err} = 0$ for public-randomness protocols whose security holds against rushing adversaries).

Let Π be as in Theorem C.1. We assume for ease of notation that an honest party that runs more than one round outputs $\perp$ (it will be clear that the attack, described below, does not benefit from this change). Finally, we omit the security parameter from the parties' input list, it will be clear though that the adversaries we present are efficient with respect to the security parameter.

Lemma C.2 (Neighboring executions)**.** *Let $\boldsymbol{v}, \boldsymbol{v}' \in \{0,1\}^n$ be with $\operatorname{dist}(\boldsymbol{v}, \boldsymbol{v}') \leq t$. Then for both $b \in \{0,1\}$:*

$$\Pr\left[\Pi(\boldsymbol{v}') \in \{b, \perp\}^n \setminus \{\perp^n\}\right] \geq \Pr\left[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n\right] - (1 - \gamma) - 4\alpha - \mathsf{err}.$$

Namely, the lemma bounds from below the probability that in a random honest execution of the protocol on input $\boldsymbol{v}'$, at least one party halts in the first round while outputting b.

We prove Lemma C.2 below, but first use it to prove Theorem C.1. We also make use of the following immediate observation.

Claim C.3 (Supermajority execution)**.** *Let $\boldsymbol{v} \in \{0,1\}^n$ and $b \in \{0,1\}$ be such that $\operatorname{dist}(\boldsymbol{v}, b^n) \leq t$. Then, $\Pr\left[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n\right] \geq 1 - \alpha - \beta$.*

Proof. Let $\mathcal{A} \subset [n]$ be a subset of size $n - t$ such that $\boldsymbol{v}_{\mathcal{A}} = b^{|\mathcal{A}|}$. The claimed validity of Π yields that

$$\Pr\left[\Pi(\boldsymbol{v})_{\mathcal{A}} \notin \{b, \perp\}^{|\mathcal{A}|}\right] < \beta.$$

This follows from β-validity of Π and the fact that an honest party cannot distinguish between an execution of $\Pi(\boldsymbol{v})$ and an execution of $\Pi(b^n)$ in which all parties not in $\mathcal{A}$ act as if their input bit is as in $\boldsymbol{v}$. Hence, by the claimed agreement of Π

$$\Pr\left[\Pi(\boldsymbol{v}) \notin \{b, \perp\}^n\right] < \alpha + \beta.$$

$\square$

Proof of Theorem C.1. We separately prove the theorem for $t \geq n/3$ and for $t \geq n/4$.

The case $t \geq n/3$. We assume for simplicity that $(n-t)/2 \in \mathbb{N}$, let $\boldsymbol{v}_0 = 0^t 1^{\lceil (n-t)/2 \rceil} 0^{\lfloor (n-t)/2 \rfloor}$ and let $\boldsymbol{v}_1 = 1^t 1^{\lceil (n-t)/2 \rceil} 0^{\lfloor (n-t)/2 \rfloor}$. Note that $\operatorname{dist}(\boldsymbol{v}_0, \boldsymbol{v}_1) = t$, and that for both $b \in \{0,1\}$ it holds that $\operatorname{dist}(\boldsymbol{v}_b, b^n) \leq t$. Hence, by Claim C.3, for both $b \in \{0,1\}$:

$$\Pr\left[\Pi(\boldsymbol{v}_b) \in \{b, \perp\}^n\right] \geq 1 - \alpha - \beta. \tag{8}$$

Applying Lemma C.2 to $\boldsymbol{v} = \boldsymbol{v}_0$ and $\boldsymbol{v}' = \boldsymbol{v}_1$ yields that

$$\Pr\left[\Pi(\boldsymbol{v}_1) \in \{0, \perp\}^n \setminus \{\perp^n\}\right] \geq 1 - 5\alpha - \beta - (1-\gamma) - \mathsf{err},$$

yielding that $5\alpha + 2\beta + (1-\gamma) + \mathsf{err} \geq 1$.

The case $t \geq n/4$. In this case there are no two vectors that are t apart in Hamming distance, and still each of them has $n-t$ entries of opposite values. Rather, we consider the two vectors $\boldsymbol{v}_0 = 0^t 0^t 0^t 1^{n-3t}$ and $\boldsymbol{v}_1 = 1^t 1^t 0^t 1^{n-3t}$ of distance $2t$. For both $b \in \{0,1\}$, the vector $\boldsymbol{v}_b$ has at least $n-t$ entries with b and is of distance t from the vector $\mathbf{v}^\star = 1^t 0^t 0^t 1^{n-3t}$.

As in the first part of the proof, Applying Claim C.3 and Lemma C.2 on $\boldsymbol{v}_b$ and $\mathbf{v}^\star$, for both $\boldsymbol{v}_1 \in \{0,1\}$, yields that

$$\Pr\left[\Pi(\mathbf{v}^\star) \in \{b, \perp\}^n \setminus \{\perp^n\}\right] \geq 1 - 5\alpha - \beta - (1-\gamma) - \mathsf{err},$$

yielding that $2(5\alpha + \beta + (1-\gamma) + \mathsf{err}) \geq 1$. $\square$

C.1 Proving Lemma C.2

Proof of Lemma C.2. Fix $b \in \{0,1\}$ and let $\delta = \Pr\left[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n\right]$. Let $\mathcal{P}$ be the coordinates in which $\boldsymbol{v}$ and $\boldsymbol{v}'$ differ, and let $\overline{\mathcal{P}} = n \setminus \mathcal{P}$. Let I be the index (a function of the parties' coins and setup parameters) of the smallest party in $\overline{\mathcal{P}}$ that halts in the first round and outputs the same value, both if the parties in $\mathcal{P}$ send their messages according to input $\boldsymbol{v}$ and if they do that according to $\boldsymbol{v}'$. We let $I = 0$ if there is no such party, and (abusing notation) sometimes identify I with the event that $I \neq 0$, e.g., $\Pr[I]$ stands for $\Pr[I \neq 0]$. Clearly,

$$\delta \leq \Pr\left[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n \quad \wedge \quad I\right] + (1 - \Pr[I])$$

and thus

$$\Pr\left[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n \quad \wedge \quad I\right] \geq \delta - (1 - \Pr[I]). \tag{9}$$

It follows that

$$\begin{aligned}
\Pr\left[\Pi(\boldsymbol{v}') \in \{b,\perp\}^n \setminus \{\perp^n\}\right] &\geq \Pr\left[\Pi(\boldsymbol{v}') \in \{b,\perp\}^n \quad \wedge \quad I\right] \\
&= \Pr\left[\Pi(\boldsymbol{v}') \in \{b,\perp\}^n \quad \wedge \quad \Pi(\boldsymbol{v}')_I = b\right] \\
&\geq \Pr\left[\Pi(\boldsymbol{v}')_I = b\right] - \alpha \\
&= \Pr\left[\Pi(\boldsymbol{v})_I = b\right] - \alpha \\
&\geq \Pr\left[\Pi(\boldsymbol{v}) \in \{b,\perp\}^n \wedge \Pi(\boldsymbol{v})_I = b\right] - 2\alpha \\
&= \Pr\left[\Pi(\boldsymbol{v}) \in \{b,\perp\}^n \wedge I\right] - 2\alpha \\
&\geq \delta - (1 - \Pr[I]) - 2\alpha.
\end{aligned} \tag{10}$$

The first inequality and the equalities hold by the definition of I. The second and third inequalities hold by agreement, and the last inequality holds by Equation (9). We conclude the proof showing that:

$$\Pr[I] \geq \gamma - \mathsf{err} - 2\alpha. \tag{11}$$

Let E_h be the event that each party in $\overline{\mathcal{P}}$ either does not halt when the parties in $\mathcal{P}$ act according to $\boldsymbol{v}$ or does not halt when they act according to $\boldsymbol{v}'$. Let E_a be the event that E_h does not occur, but $I = 0$ (i.e., the parties that halt in the first round, output different values according the $\mathcal{P}$ input. Clearly $I = 0 \Longleftrightarrow E_h \vee E_a$.

Consider the adversary that in the first round acts toward a random subset of $\mathcal{P}$ according to input $\boldsymbol{v}$ and towards the remaining parties according to $\boldsymbol{v}'$, and aborts at the end of this round. It is clear that if E_a occurs, the above adversary violates agreement with probability $1/2$. Thus, $\Pr[E_a] \leq 2\alpha$.

It is also clear that when E_h occurs, the above attacker fails to prevent an honest party in $\overline{\mathcal{P}}$ from halting in the first round only if the following event happens: each party in $\overline{\mathcal{P}}$ does not halt in $\Pi(\boldsymbol{v}'')$ for some $\boldsymbol{v}'' \in \{\boldsymbol{v}, \boldsymbol{v}'\}$, but the adversary acts towards each of these parties on the input in which it does halt. The latter event happen with probability at most $2^{-|\overline{\mathcal{P}}|} \leq 2^{t-n} = \mathsf{err}$. Thus, $\Pr[E_h] \leq 1 - \gamma - \mathsf{err}$. We conclude that

$$\Pr[I] \geq 1 - \Pr[E_h] - \Pr[E_a] \geq \gamma - \mathsf{err} - 2\alpha.$$

Finally, we note that if the protocol has public randomness, the (now rushing) attacker does not have to guess what input to act upon. Rather, after seeing the first round randomness, it *finds* an input $\boldsymbol{v}'' \in \{\boldsymbol{v}, \boldsymbol{v}'\}$ such that at least one party in $\overline{\mathcal{P}}$ does not halt in $\Pi(\boldsymbol{v}'')$ or violates agreement, and acts according to this input. Hence, the bound on I changes to

$$\Pr[I] \geq \gamma - \alpha,$$

proving the theorem statement for such protocols. □

D Lower Bounds on Second-Round Halting

In this section, we prove lower bounds for second-round halting of Byzantine agreement protocols. In Appendix D.1, we prove a bound for arbitrary protocols, and in Appendix D.2, we give a much stronger bound for public-randomness protocols (the natural extension of public-coin protocols to the 'with-input' setting).

D.1 Arbitrary Protocols

In this section, we prove our lower bound for second-round halting of arbitrary protocols.

Theorem D.1 (Bound on second-round halting, arbitrary protocols. Theorem B.6 restated)**.** *Let* Π *be a* PPT n*-party protocol that is a* $(t, \alpha, \beta, 2, \gamma)$-BA *against locally consistent, static, non-rushing adversaries for* $t > n/4$*. Then* $\gamma \leq 1 + 2\alpha + \frac{\beta}{w^2} - \frac{1}{2w^2}$ *for* $w = \lceil (n - \lceil n/4 \rceil)/\lfloor t - n/4 \rfloor \rceil + 1$*.*

Let Π be as in Theorem D.1. We assume for ease of notation that an honest party that runs more than two rounds outputs $\perp$ (it will be clear that the attack, described below, does not benefit from this change). We also assume without loss of generality that the honest parties in an execution of Π never halt in one round (by adding a dummy round if needed). Finally, we omit the security parameter from the parties' input list, it will be clear though that the adversaries we present are efficient with respect to the security parameter.

Let $k = \lceil n/4 \rceil$ and let $h = \lceil (n-k)/(t-k) \rceil$. The theorem is easily implied by the next lemma.

Lemma D.2 (Neighboring executions)**.** *Let* $\boldsymbol{v}, \boldsymbol{v}' \in \{0,1\}^n$ *be with* $\operatorname{dist}(\boldsymbol{v}, \boldsymbol{v}') \leq k$*. Then for every* $b \in \{0,1\}$*:*

$$\Pr\left[\Pi(\boldsymbol{v}') = b^n\right] \geq \Pr\left[\Pi(\boldsymbol{v}) = b^n\right] - h(h+1)(2\alpha + 1 - \gamma) - \alpha.$$

Namely, the lemma bounds from below the probability that in a random honest execution of the protocol on input $\boldsymbol{v}'$ all parties halt within two rounds while outputting b.

We prove Lemma D.2 below, but first use it to prove Theorem D.1. We also make use of the following immediate observation.

Claim D.3 (Supermajority execution)**.** *Let* $\boldsymbol{v} \in \{0,1\}^n$ *and* $b \in \{0,1\}$ *be such that* $\operatorname{dist}(\boldsymbol{v}, b^n) \leq t$*. Then,* $\Pr\left[\Pi(\boldsymbol{v}) = b^n\right] \geq 1 - \alpha - \beta - (1 - \gamma)$*.*

Proof. The same argument as in the proof of Claim C.3 yields that

$$\Pr\left[\Pi(\boldsymbol{v}) \notin \{b, \perp\}^n\right] < \alpha + \beta.$$

Thus, by γ-second-round halting

$$\Pr\left[\Pi(\boldsymbol{v}) \neq b^n\right] < \alpha + \beta + (1 - \gamma).$$

□

Proof of Theorem D.1. Consider the vectors $\boldsymbol{v}_0 = 0^k 0^k 0^k 1^{n-3k}$, $\boldsymbol{v}_1 = 1^k 1^k 0^k 1^{n-3k}$ and $\mathbf{v}^\star = 1^k 0^k 0^k 1^{n-3k}$. Note that for both $b \in \{0,1\}$ it holds that $\operatorname{dist}(\boldsymbol{v}_b, b^n) \leq t$ (since $n/4 \leq k \leq t$), and that $\operatorname{dist}(\boldsymbol{v}_b, \mathbf{v}^\star) = k$. Applying Lemma D.2 and Claim D.3 for each of these vectors, yields that for both $b \in \{0,1\}$:

$$\begin{aligned}
\Pr\left[\Pi(\mathbf{v}^\star) = b^n\right] &\geq 1 - \alpha - \beta - (1 - \gamma) - h(h+1)(2\alpha + 1 - \gamma) - \alpha \\
&\geq 1 - \beta - (h+1)^2(2\alpha + 1 - \gamma).
\end{aligned}$$

Note that $w = h + 1$, which implies $\beta + w^2(2\alpha + 1 - \gamma) \geq 1/2$, and the proof follows by a simple calculation. □

D.1.1 Proving Lemma D.2

We assume for ease of notation that $\operatorname{dist}(\boldsymbol{v}, \boldsymbol{v}') = k$ (and not $\leq k$). Let $\ell = \lfloor \varepsilon_t n \rfloor$ (hence, $h = \lceil (n-k)/\ell \rceil$). Assume for ease of notation that $h \cdot \ell = n - k$ (i.e., no rounding), and for a k-sized subset of parties $\mathcal{P} \subset [n]$, let $\mathcal{L}_1^{\mathcal{P}}, \ldots, \mathcal{L}_h^{\mathcal{P}}$ be an arbitrary partition of $\overline{\mathcal{P}} = [n] \setminus \mathcal{P}$ into ℓ-sized subsets. Consider the following family of protocols:

Protocol D.4 ($\Pi_d^{\mathcal{P}}$)**.**

Parameters: *A subset $\mathcal{P} \subseteq [n]$ and an index $d \in (h)$.*

Input: *Every party P_i has an input bit $v_i \in \{0,1\}$.*

First round:

Party $\mathsf{P}_i \in \mathcal{P}$. *If $d = 0$ [resp., $d = h$], act honestly according to Π with respect to input bit v_i [resp., $1 - v_i$]. Otherwise,*

1. *Choose random coins honestly (i.e., uniformly at random).*
2. *To each party in $\bigcup_{j \in \{1,\ldots,d\}} \mathcal{L}_j^{\mathcal{P}}$: send a message according to input $1 - v_i$.*
3. *To each party in $\bigcup_{j \in \{d+1,\ldots,h\}} \mathcal{L}_j^{\mathcal{P}}$: send a message according to input v_i (real input).*
4. *Send no messages to the other parties in $\mathcal{P}$.*

Other parties. *Act according to Π.*

Second round:

Party $\mathsf{P}_i \in \mathcal{P}$. *If $d = 0$ [resp., $d = h$], act honestly according to Π with respect to input bit v_i [resp., $1 - v_i$]; otherwise, abort.*

Other parties. *Act honestly according to Π.*

Namely, the "pivot" parties in $\mathcal{P}$ gradually shift their inputs from their real input to its negation according to parameter d. Note that protocol $\Pi_0^{\mathcal{P}}(\boldsymbol{v})$ is equivalent to an honest execution of protocol $\Pi(\boldsymbol{v})$, and $\Pi_h^{\mathcal{P}}(\boldsymbol{v})$ is equivalent to an honest execution of $\Pi(\boldsymbol{v}')$, for $\boldsymbol{v}'$ being $\boldsymbol{v}$ with the coordinates in $\mathcal{P}$ negated. Lemma D.2 easily follows by the next claim about Protocol D.4. In the following we let $\delta = \Pr\left[\Pi(\boldsymbol{v})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|}\right]$.

Claim D.5. *For any k-sized subset $\mathcal{P} \subset [n]$ and $d \in (h)$ it holds that*

$$\Pr\left[\Pi_d^{\mathcal{P}}(\boldsymbol{v})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|}\right] \geq \delta - d(h+1)(2\alpha + 1 - \gamma).$$

We prove Claim D.5 below, but first use it to prove Lemma D.2.

Proof of Lemma D.2. By Claim D.5

$$\Pr\left[\Pi_h^{\mathcal{P}}(\boldsymbol{v})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|}\right] \geq \delta - h(h+1)(2\alpha + 1 - \gamma).$$

Since $\Pi_h^{\mathcal{P}}(\boldsymbol{v})$ is just an honest execution of $\Pi(\boldsymbol{v}')$, by agreement

$$\Pr\left[\Pi(\boldsymbol{v}') = b^n\right] \geq \delta - h(h+1)(2\alpha + 1 - \gamma) - \alpha.$$

□

Proof of Claim D.5. The proof is by induction on d. The base case $d = 0$ holds by definition. Suppose for contradiction the claim does not hold, and let $d^* \in (h-1)$ be such that the claim holds for d^* but not for d^*+1. Let γ_d be the probability that all honest parties halt in the second round of a random execution of $\Pi_d^{\mathcal{P}}(\boldsymbol{v})$. The assumption about d^* yields that

$$\Pr\left[\Pi_{d^*}^{\mathcal{P}}(\boldsymbol{v})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|}\right] \geq \delta - \beta - d^*(h+1)(2\alpha + 1 - \gamma) \tag{12}$$

and

$$\Pr\left[\Pi_{d^*+1}^{\mathcal{P}}(\boldsymbol{v})_{\overline{\mathcal{P}}} \in \{0,1\}^{|\overline{\mathcal{P}}|} \setminus \{b^{|\overline{\mathcal{P}}|}\}\right] > 1 - (\delta - \beta - (d^*+1)(h+1)(2\alpha+1-\gamma)) - (1-\gamma_d) \tag{13}$$

We note that for every $d \in (h)$

$$\frac{1-\gamma_d}{h+1} \leq 1 - \gamma \tag{14}$$

Indeed, otherwise, the adversary that corrupts the parties in $\mathcal{P}$ and acts like $\Pi_d^{\mathcal{P}}$ for a random $d \in (h)$, violates the γ-second-round-halting property of Π. (The reader is reminded that we denote by (h) the set $\{0, 1, \ldots, h\}$) We conclude that

$$\begin{aligned}
&\Pr_{\boldsymbol{r}}\left[\Pi_{d^*}^{\mathcal{P}}(\boldsymbol{v};\boldsymbol{r})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|} \quad \wedge \quad \Pi_{d^*+1}^{\mathcal{P}}(\boldsymbol{v};\boldsymbol{r})_{\overline{\mathcal{P}}} \in \{0,1\}^{|\overline{\mathcal{P}}|} \setminus \{b^{|\overline{\mathcal{P}}|}\}\right] \\
&\geq 1 - \left(1 - \Pr_{\boldsymbol{r}}\left[\Pi_{d^*}^{\mathcal{P}}(\boldsymbol{v};\boldsymbol{r})_{\overline{\mathcal{P}}} = b^{|\overline{\mathcal{P}}|}\right]\right) - \left(1 - \Pr_{\boldsymbol{r}}\left[\Pi_{d^*+1}^{\mathcal{P}}(\boldsymbol{v};\boldsymbol{r})_{\overline{\mathcal{P}}} \in (\{0,1\}^{|\overline{\mathcal{P}}|} \setminus \{b^{|\overline{\mathcal{P}}|}\}\right]\right) \\
&> (h+1)(2\alpha + 1 - \gamma) - (1 - \gamma_d) \\
&\geq (h+1)2\alpha.
\end{aligned} \tag{15}$$

for $\boldsymbol{r}$ being the randomness of the parties. The first inequality is by Equations (12) and (13), and the second one by Equation (14).

Consider the adversary that samples $d \leftarrow (h)$, corrupts the parties in $\mathcal{P} \cup \mathcal{L}_{d+1}^{\mathcal{P}}$, and acts towards a uniform random subset of the honest parties according to $\Pi_d^{\mathcal{P}}$ and to the remaining parties according to $\Pi_{d+1}^{\mathcal{P}}$. Equation (15) yields that the above adversary causes disagreement with probability larger than $(h+1)2\alpha/2(h+1) = \alpha$. Since it corrupts at most t parties, this contradicts the assumption about Π. □

D.2 Public-Randomness Protocols

In this section, we prove our lower bound for second-round halting of public-randomness protocols.

Theorem D.6 (Lower bound on second-round halting, public-randomness protocols. Theorem B.7 restated)**.** *Assume Conjecture B.8 holds. Then, for any $\varepsilon_t, \varepsilon_\gamma > 0$ there exists $\alpha > 0$ such that the following holds for large enough n: let Π be a* PPT *n-party, public-randomness protocol that is $(t, \alpha, \beta = \varepsilon_\gamma^2/200, 2, \gamma)$-*BA *against locally consistent, rushing, adaptive adversaries. Then,*

- *$t \geq (1/3 + \varepsilon_t)n$ implies $\gamma < \varepsilon_\gamma$.*
- *$t \geq (1/4 + \varepsilon_t)n$ implies $\gamma < \frac{1}{2} + \varepsilon_\gamma$.*

Assume Conjecture B.8 holds. Let Π be as in the theorem statement, and assume $\gamma = \varepsilon_\gamma$ in the case $t \geq (1/3+\varepsilon_t)n$ and $\gamma = \frac{1}{2}+\varepsilon_\gamma$ in the case $t \geq (1/4+\varepsilon_t)n$. We prove that in both cases α, the agreement error, has to be larger than some universal constant depending only on ε_t and ε_γ.

Let $\lambda = \varepsilon_\gamma/10$ and $\sigma = \varepsilon_t/4$. Recall that $\perp_{\mathcal{S}}(x)$ is defined by $\perp_{\mathcal{S}}(x)_i = \begin{cases} \perp, & i \in \mathcal{S}, \\ x_i, & \text{otherwise.} \end{cases}$. Conjecture B.8 yields that there exists $\delta > 0$ such that the following holds for large enough n: let Σ be a finite alphabet and let $\mathcal{A}_0, \mathcal{A}_1 \subset \{\Sigma \cup \perp\}^n$ be two sets such that for both $b \in \{0,1\}$:

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \Sigma^n}\left[\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b\right] \geq \lambda\right] \geq 1-\delta.$$

Then,

$$\Pr_{\boldsymbol{r} \leftarrow \Sigma^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\forall b \in \{0,1\}\colon\ \{\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b \neq \emptyset\right] \geq \delta \tag{16}$$

We assume that $\alpha = \min\{\delta\lambda\varepsilon_t/10, \beta = \lambda^2/2\}$ and derive a contradiction. Fix n that is large enough for Equation (16) to hold and that $\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}[|\mathcal{S}| > 2\sigma n] = 2^{-\Theta(n \cdot \sigma^2)} \leq \alpha$, i.e., $n > \Theta(\log 1/\alpha)/\sigma^2)$.

As in the proof of Theorem D.1, we assume for ease of notation that an honest party that runs more than two round outputs $\perp$, and that the honest parties in Π never halt in one round. We also omit the security parameter from the parties input list. We assume without loss of generality that in the first round, the party flips no coin, since such coins can be added to the setup parameter.

We use the following notation: the setup parameter and second round randomness of the parties in Π are identified with elements of $\mathcal{F}$ and $\mathcal{R}$, respectively. We denote by f_i and r_i the setup parameter and the second part randomness of party P_i in Π, and let $D_{\mathcal{F}}$ be the joint distribution of the parties setup parameters (by definition, the joint distribution of the second round randomness is the product distribution $\mathcal{R}^n$). For $\boldsymbol{v} \in \{0,1\}^n$, $\boldsymbol{f} = (f_1, \ldots, f_n) \in \operatorname{Supp}(D_{\mathcal{F}})$ and $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathcal{R}^n$, let $\Pi(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))$ denote the execution of Π in which party P_i gets input v_i, setup parameter f_i and second-round randomness r_i. We naturally apply this notation for the variants of Π considered in the proof.

For $\mathcal{S} \subseteq [n]$, let $\Pi^{\mathcal{S}}$ be the variant of Π in which the parties in $\mathcal{S}$ halt at the end of the first round. Let $k = \lceil t - \varepsilon_t \cdot n \rceil$ (i.e., $k = \lceil n/3 \rceil$ if $t \geq (1/3+\varepsilon_t)n$, and $k = \lceil n/4 \rceil$ if $t \geq (1/4+\varepsilon_t)n$). The heart of the proof lies in the following lemma.

Lemma D.7 (Neighboring executions)**.** *Let $\boldsymbol{v}, \boldsymbol{v}' \in \{0,1\}^n$ be with $\operatorname{dist}(\boldsymbol{v}, \boldsymbol{v}') \leq k$, let $b \in \{0,1\}$ and let $\overline{\mathcal{S}} = [n] \setminus \mathcal{S}$. Then with probability at least $\gamma - 7\lambda - \frac{\alpha + \Pr[\Pi(\boldsymbol{v}) \neq b^n]}{\lambda}$ over $\boldsymbol{f} \leftarrow D_{\mathcal{F}}$, it holds that*

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\Pi(\boldsymbol{v}'; (\boldsymbol{f}, \boldsymbol{r})) = b^n \quad \wedge \quad \Pi^{\mathcal{S}}(\boldsymbol{v}'; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{S}}} = b^{|\overline{\mathcal{S}}|}\right] \geq \lambda\right] \geq 1-\delta$$

Namely, in an execution of $\Pi(\boldsymbol{v}')$, all honest parties halt after two rounds and output b, regardless of whether a random subset of parties aborts after the first round. Lemma D.7 is proven in Appendix D.2.1, but let us first use it to prove Theorem B.7. We make use of the following immediate observation:

Claim D.8 (Supermajority execution)**.** *Let $\boldsymbol{v} \in \{0,1\}^n$ and $b \in \{0,1\}$ be such that $\operatorname{dist}(\boldsymbol{v}, b^n) \leq t$. Then $\Pr[\Pi(\boldsymbol{v}) \in \{b, \perp\}^n] \geq 1 - \alpha - \beta$.*

Proof. The proof of this claim uses an identical argument as in the proof of Claim C.3. □

Proving Theorem B.7.

Proof of Theorem B.7. We separately prove the case $t \geq (1/3+\varepsilon_t)n$ and $t \geq (1/4+\varepsilon_t)n$.

The case $t \geq (1/3+\varepsilon_t)n$. Let $\boldsymbol{v}_0 = 0^k 1^{\lceil (n-k)/2 \rceil} 0^{\lfloor (n-k)/2 \rfloor}$ and let $\boldsymbol{v}_1 = 1^k 1^{\lceil (n-k)/2 \rceil} 0^{\lfloor (n-k)/2 \rfloor}$. Note that $\operatorname{dist}(\boldsymbol{v}_0, \boldsymbol{v}_1) = k$ and that for both $b \in \{0,1\}$ it holds that $\operatorname{dist}(\boldsymbol{v}_b, b^n) \leq t$. We will use Lemma D.7 and Claim D.8 to prove that $\Pi(\boldsymbol{v}_1) = 0^n$ with noticeable probability, contradicting the validity of the protocol.

Recall that $\lambda = \varepsilon_\gamma/8$ and $\alpha, \beta \leq \lambda^2/2$. Claim D.8 yields that for both $b \in \{0,1\}$:

$$\Pr\left[\Pi(\boldsymbol{v}_b) \in \{b, \perp\}^n\right] \geq 1 - \alpha - \beta \geq 1 - \lambda^2 \tag{17}$$

Applying Lemma D.7 with respect to $\boldsymbol{v}_0$, yields that with probability at least λ over $\boldsymbol{f} \leftarrow D_{\mathcal{F}}$:

$$\Pr_{\boldsymbol{r}}\left[\Pi(\boldsymbol{v}_1; (\boldsymbol{f}, \boldsymbol{r})) = 0^n\right] \geq \lambda$$

and therefore

$$\Pr\left[\Pi(\boldsymbol{v}_1) = 0^n\right] \geq 2\lambda^2$$

in contradiction to Equation (17).

The case $t \geq (1/4+\varepsilon_t)n$. Consider the vectors $\boldsymbol{v}_0 = 0^k 0^k 0^k 1^{n-3k}$, $\boldsymbol{v}_1 = 1^k 1^k 0^k 1^{n-3k}$ and $\mathbf{v}^\star = 1^k 0^k 0^k 1^{n-3k}$. Note that for both $b \in \{0,1\}$ it holds that $\operatorname{dist}(\boldsymbol{v}_b, b^n) \leq t$ and that $\operatorname{dist}(\boldsymbol{v}_b, \mathbf{v}^\star) = k$. Applying Lemma D.7 and Claim D.8 on $\boldsymbol{v}_b$ and $\mathbf{v}^\star$, for both $b \in \{0,1\}$, yields that $\Pi^{\mathcal{S}}(\mathbf{v}^\star) = b^n$ with noticeable probability. This will allow us to use Conjecture B.8 to lowerbound the protocol's agreement.

A similar calculation to that done in the $t \geq (1/3+\varepsilon_\gamma)n$ part yields that by Lemma D.7 and Claim D.8, for both $b \in \{0,1\}$: with probability at least $\frac{1}{2} + 2\lambda$ over $\boldsymbol{f} \leftarrow D_{\mathcal{F}}$ it holds that

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\Pi(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r})) = b^n \quad \wedge \quad \Pi^{\mathcal{S}}(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{S}}} = b^{\left|\overline{\mathcal{S}}\right|}\right] \geq \lambda\right] \geq 1 - \delta$$

It follows that there exists a set $\mathcal{T} \subseteq \operatorname{Supp}(D_{\mathcal{F}})$ with $\Pr_{\boldsymbol{f} \leftarrow D_{\mathcal{F}}}[\mathcal{T}] \geq 4\lambda$, such that for every $\boldsymbol{f} \in \mathcal{T}$, for *both* $b \in \{0,1\}$:

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\Pi(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r})) = b^n \quad \wedge \quad \Pi^{\mathcal{S}}(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{S}}} = b^{\left|\overline{\mathcal{S}}\right|}\right] \geq \lambda\right] \geq 1 - \delta \tag{18}$$

We assume without loss of generality that if a party gets $\perp$ as its second-round random coins, it aborts after the first round. For $\boldsymbol{r} \in \{\mathcal{R} \cup \perp\}$, let $\mathcal{E}(\boldsymbol{r})$ be the indices of the $\perp$'s in $\boldsymbol{r}$. For $\boldsymbol{f} \in \operatorname{Supp}(D_{\mathcal{F}})$ and $b \in \{0,1\}$, let

$$\mathcal{A}_b^{\boldsymbol{f}} = \left\{\boldsymbol{r} \in \{\mathcal{R} \cup \perp\} : \Pi(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{E}(\boldsymbol{r})}} = b^{\left|\overline{\mathcal{E}(\boldsymbol{r})}\right|}\right\} \tag{19}$$

By Equation (18), for $\boldsymbol{f} \in \mathcal{T}$ and $b \in \{0,1\}$, it holds that

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b^{\boldsymbol{f}}\right] \geq \lambda\right] \geq 1 - \delta \tag{20}$$

Hence by Conjecture B.8, see Equation (16), for $\boldsymbol{f} \in \mathcal{T}$ it holds that

$$\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} [\forall b \in \{0,1\} \colon \{\boldsymbol{r}, \bot_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b \neq \emptyset] > \delta$$

That is,

$$\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} \left[\forall b \in \{0,1\} \quad \exists \mathcal{S}_b \in \{\mathcal{S}, \emptyset\} : \Pi^{\mathcal{S}_b}(\mathbf{v}^\star; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{S}_b}} = b^{\left|\overline{\mathcal{S}_b}\right|}\right] > \delta \tag{21}$$

Consider the following adversary:

Algorithm D.9 (A)**.**

Pre-interaction. *Corrupt a random subset* $\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}$ *conditioned on* $|\mathcal{S}| \leq 2\sigma n$*.*

First round. *Act according to* Π*.*

Second round. *Sample* $\mathcal{S}_0, \mathcal{S}_1$ *at random from* $\{\emptyset, \mathcal{S}\}$*, and act towards some honest parties according to* $\Pi^{\mathcal{S}_0}$ *and towards the others according to* $\Pi^{\mathcal{S}_1}$ *.*

By Equation (21), the above adversary violates the agreement of Π on input $\mathbf{v}^\star$ with probability larger than $\delta - \Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}[|\mathcal{S}| > 2\sigma n] > \alpha$, in contradiction with the assumed agreement of Π. $\square$

D.2.1 Proving Lemma D.7

We assume for simplicity that $\mathrm{dist}(\boldsymbol{v}, \boldsymbol{v}') = k$ (and not $\leq k$). Let $\ell = \lfloor (t-k)/2 \rfloor$ and let $h = \lceil (n-k)/\ell \rceil$. Assume for ease of notation that $h \cdot \ell = n - k$ (i.e., no rounding), and for k-size subset of parties $\mathcal{P} \subset [n]$, let $\mathcal{L}_1^{\mathcal{P}}, \ldots, \mathcal{L}_h^{\mathcal{P}}$ be an arbitrary partition of $\overline{\mathcal{P}} = [n] \setminus \mathcal{P}$ into ℓ-size subsets. Consider the following protocol family.

Protocol D.10 ($\Pi_d^{\mathcal{P},\mathcal{S}}$).

Parameters: *subsets $\mathcal{P},\mathcal{S} \subseteq [n]$ and index $d \in (h)$.*

Input: *Party P_i has setup parameter f_i and input bit v_i.*

First one:

> **Party $\mathsf{P}_i \in \mathcal{P}$.** *If $d = 0$ [resp., $d = h$], act honestly according to Π with respect to input bit v_i [resp., $1 - v_i$]. Otherwise,*
>
> 1. *Choose random coins honestly (i.e., uniformly at random).*
> 2. *To each party in $\bigcup_{i \in \{1,\ldots,d\}} \mathcal{L}_j^{\mathcal{P}}$: send message according to input $1 - v_i$.*
> 3. *To each party in $\bigcup_{i \in \{d+1,\ldots,h\}} \mathcal{L}_j^{\mathcal{P}}$: send message according to input v_i (real input).*
> 4. *Send no messages to the other parties in $\mathcal{P}$.*
>
> **Other parties.** *Act according to Π.*

Second round:

> **Parties in $\mathcal{P} \setminus \mathcal{S}$.** *If $d = 0$ [resp., $d = h$], act honestly according to Π with respect to input bit v_i [resp., $1 - v_i$]; otherwise, abort.*
>
> **Parties in $\mathcal{S}$.** *Abort.*
>
> **Other parties.** *Act according to Π.*

Namely, the "pivot" parties in $\mathcal{P}$ shift their inputs from their real input to the flipped one according to parameter d. The "aborting" parties in $\mathcal{S}$ abort at the end of the first round. Note that protocol $\Pi_0^{\mathcal{P},\mathcal{S}}$ is the same as protocol $\Pi^{\mathcal{S}}$, and $\Pi_h^{\mathcal{P},\mathcal{S}}(\boldsymbol{v})$ acts like $\Pi^{\mathcal{S}}(\boldsymbol{v}')$, for $\boldsymbol{v}'$ being $\boldsymbol{v}$ with the coordinates in $\mathcal{P}$ flipped. In the following we let $\Pi_d = \Pi_d^{\emptyset}$.

For $\mathcal{P},\mathcal{S} \subseteq [n]$, $d \in (h)$ and $c \in \{0,1\}$, let

$$\mathcal{V}_{d,c}^{\mathcal{P}} = \left\{ (\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}) \colon \quad \Pi_d^{\mathcal{P},\mathcal{S}}(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{S}}} = c^{\left|\overline{\mathcal{P} \cup \mathcal{S}}\right|} \right\}.$$

letting $\overline{\mathcal{P} \cup \mathcal{S}} = [n] \setminus (\mathcal{P} \cup \mathcal{S})$. Namely, $\mathcal{V}_{d,c}^{\mathcal{P}}$ are the sets, setup parameters and random strings on which honest parties in $\Pi_d^{\mathcal{P},\mathcal{S}}$ halt in the second-round and output c. Let $\chi = \Pr\left[\Pi(\boldsymbol{v}) \neq b^n\right]$ and let

$$\mathcal{T}_{d,c} = \left\{ \boldsymbol{f} \colon \Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} \left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n} \left[(\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}), (\boldsymbol{f}, \emptyset, \boldsymbol{r}) \in \mathcal{V}_{d,c} \right] \geq \lambda \right] \geq 1 - \delta \right\}$$

The proof of Lemma D.7 immediately follows by the next lemma.

Lemma D.11. *For every k-size subset $\mathcal{P} \subset [n]$ and $d \in [h]$, it holds that*

$$\Pr\left[\mathcal{T}_{d,b}\right] \geq \gamma - 7\lambda - \frac{\chi + \alpha}{\lambda}.$$

Proof of Lemma D.7. Immediate by Lemma D.11. □

The rest of this subsection is devoted for proving Lemma D.11. Fix a k-size subset $\mathcal{P} \subset [n]$ and omit it from the notation when clear from the context. Let

$$\widetilde{\mathcal{V}}_{d,c} = \left\{ (\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}) \colon \forall a \in \{0,1\} \quad \Pi^{\mathcal{P},\mathcal{S}}_{d+a}(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{S}}} = c^{\left|\overline{\mathcal{P} \cup \mathcal{S}}\right|} \right\}.$$

Namely, $\widetilde{\mathcal{V}}_{d,c}$ are the sets, setup parameters and random strings on which honest parties in $\Pi^{\mathcal{P},\mathcal{S}}_{d+a}$ halt in the second-round and output c, *regardless* whether the parties in $\mathcal{S}$ aborts *and* whether the parties in $\mathcal{P}$ act toward those in $\mathcal{L}_{d+1}$ according to input 0 or 1. Let

$$\widetilde{\mathcal{T}}_{d,c} = \left\{ \boldsymbol{f} \colon \Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}} \left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n} \left[(\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}), (\boldsymbol{f}, \emptyset, \boldsymbol{r}) \in \widetilde{\mathcal{V}}_{d,c} \right] \geq \lambda \right] \geq 1 - \delta \right\},$$

let $\widetilde{\mathcal{T}}_d = \widetilde{\mathcal{T}}_{d,0} \cup \widetilde{\mathcal{T}}_{d,1}$ and let $\widetilde{\mathcal{T}} = \bigcap_{i \in (h-1)} \widetilde{\mathcal{T}}_d$. Lemma D.11 is proved via the following claims (following probabilities are taken over $\boldsymbol{f} \leftarrow D_{\mathcal{F}}$).

Claim D.12. $\Pr\left[\widetilde{\mathcal{T}}\right] \geq \gamma - 6\lambda$.

Claim D.13. $\Pr\left[\mathcal{T}_{1,b} \mid \widetilde{\mathcal{T}}\right] \geq 1 - \frac{\chi+\alpha}{\Pr\left[\widetilde{\mathcal{T}}\right] \cdot \lambda}$.

Claim D.14. $\Pr\left[\mathcal{T}_{d+1,b} \mid \widetilde{\mathcal{T}}\right] < \eta$ *implies* $\Pr\left[\mathcal{T}_{d,\overline{b}} \mid \widetilde{\mathcal{T}}\right] \geq 1 - \eta$.

Proof. Immediate by the definitions of $\widetilde{\mathcal{T}}$ and $\mathcal{T}$. □

Claim D.15. $\Pr\left[\mathcal{T}_{d,0} \mid \widetilde{\mathcal{T}}\right] + \Pr\left[\mathcal{T}_{d,1} \mid \widetilde{\mathcal{T}}\right] \leq 1 + \lambda/(h \cdot \Pr[\widetilde{\mathcal{T}}])$ *for every* $d \in [h-1]$.

We prove Claims D.12, D.13 and D.15 below, but first use the above claims for proving Lemma D.7.

Proving Lemma D.11.

Proof of Lemma D.11. We first prove that for every $d \in [h]$:

$$\Pr\left[\mathcal{T}_{d,b} \mid \widetilde{\mathcal{T}}\right] \geq 1 - \frac{\delta + \chi}{\Pr\left[\widetilde{\mathcal{T}}\right] \cdot \lambda} - \frac{d\lambda}{h \cdot \Pr[\widetilde{\mathcal{T}}]}.$$

The proof is by induction on d. The base case $d = 1$ is by Claim D.13, and the induction follows by the combination of Claims D.14 and D.15. Applying the above for $d = h$, we get that

$$\Pr\left[\mathcal{T}_{h,b}\right] \geq \Pr\left[\widetilde{\mathcal{T}}\right] - \frac{\delta + \chi}{\lambda} - \lambda, \tag{22}$$

and the proof follows by Claim D.12. □

So it is left to prove Claims D.12, D.13 and D.15. Note that the following adversaries corrupt at most $k + \ell + 2\sigma n \leq t$ and thus they make a valid attack. Since our security model consider rushing adversaries, and Π is pubic randomness, we assume the adversary knows $\boldsymbol{f} = (f_1, \ldots, f_n)$ *before* sending its first round messages.

Proving Claim D.12. This is the only part in proof where we exploit the fact that the protocol is secure against adaptive adversaries.

Proof of Claim D.12. Consider the following *rushing adaptive* adversary.

Algorithm D.16 (A)**.**

Pre interaction:

Corrupt the parties in $\mathcal{P}$*.*

First round.

Let $\boldsymbol{f}$ *be the parties' setup parameters.*

Do $1/\lambda\delta$ *times:*

1. *Sample* $\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}$ *conditioned on* $|\mathcal{S}| \leq 2\sigma n$*.*
2. *For each* $i \in (h-1)$*: estimate* $\xi_i = \Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[(\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}), (\boldsymbol{f}, \emptyset, \boldsymbol{r}) \in \widetilde{\mathcal{V}}_i\right]$ *by taking* $\Theta(\log(h/\lambda))$ *samples of* $\boldsymbol{r}$*.*
3. *Let* $d = \operatorname{argmin}_{i \in (h-1)} \{\xi_i\}$*.*
4. *If* $\xi_d < 2\lambda$*, break the loop.*

Corrupt the parties in $\mathcal{S} \cup \mathcal{L}_{d+1}$*, and act according to* Π_d*.*

Second round.

Let $\boldsymbol{r}$ *be the parties' second round randomness.*

If $(\boldsymbol{f}, \emptyset, \boldsymbol{r}) \notin \mathcal{V}_{d+a}$ *for some* $a \in \{0, 1\}$*,*

act according to Π_{d+a}*.*

Else,

Let $a \in \{0, 1\}$ *be such that* $(\boldsymbol{f}, \mathcal{S}, \boldsymbol{r}) \notin \mathcal{V}_{d+a}$*, set to* 0 *if not such value exists.*

Act according to $\Pi_{d+a}^{\mathcal{S}}$*.*

. . . .

Let D be the value of d chosen by A (at the first round of the protocol). Since $\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}[|\mathcal{S}| > 2\sigma n] \leq \alpha < \delta/2$, if $\boldsymbol{f} \notin \widetilde{\mathcal{T}}$ then except with probability λ it holds that $\xi_D \leq 2\lambda$. Where if $\xi_D \leq 2\lambda$, then in the interaction with A the honest parties both halt in the second round and output the same value with probability at most 5λ. Where since $\alpha < \lambda$, the honest parties halt in the second round of such interaction with probability smaller than 6λ. We conclude that the honest parties halt in the second round under the above attack with probability smaller than $\Pr\left[\widetilde{\mathcal{T}}\right] + \Pr\left[\neg\widetilde{\mathcal{T}}\right] \cdot 6\lambda \leq \Pr\left[\widetilde{\mathcal{T}}\right] + 6\lambda$, yielding that $\Pr\left[\widetilde{\mathcal{T}}\right] > \gamma - 6\lambda$. $\square$

Proving Claim D.13.

Proof of Claim D.13. By definition, for $\boldsymbol{f} \in \mathcal{T}_{1,b}$ it holds that

$$\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\Pi_1(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{H}}} = \bar{b}^{|\overline{\mathcal{H}}|}\right] = \Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[(\boldsymbol{f}, \emptyset, \boldsymbol{r}) \in \mathcal{V}_{1,\bar{b}}\right] \geq \lambda$$

letting $\mathcal{H} = \mathcal{P} \cup \mathcal{L}_1$ and $\overline{\mathcal{H}} = [n] \setminus \mathcal{H}$. Let $\eta = \Pr_{\boldsymbol{f}}\left[\mathcal{T}_{1,\bar{b}} \mid \widetilde{\mathcal{T}}\right]$, clearly, $\Pr_{\boldsymbol{f}}\left[\mathcal{T}_{1,b} \mid \widetilde{\mathcal{T}}\right] = 1 - \eta$. By the above

$$\Pr\left[\Pi_1(\boldsymbol{v})_{\overline{\mathcal{H}}} = \bar{b}^{|\overline{\mathcal{H}}|}\right] \geq \Pr\left[\widetilde{\mathcal{T}}\right] \cdot \eta \cdot \lambda \tag{23}$$

Finally, we notice that

$$\Pr\left[\Pi_1(\boldsymbol{v}) = \bar{b}^{|\mathcal{H}|}\right] + \Pr\left[\Pi(\boldsymbol{v}) = b^n\right] \leq 1 + \alpha \tag{24}$$

Otherwise, the adversary corrupting the parties in $\mathcal{H}$, and acting toward the first honest parties according to Π and toward the rest according to Π_1 violates the α-agreement of Π. We conclude that $\Pr\left[\widetilde{\mathcal{T}}\right] \cdot \eta \cdot \lambda \leq \chi + \alpha$, and therefore $\eta \leq \frac{\chi+\alpha}{\Pr\left[\widetilde{\mathcal{T}}\right] \cdot \lambda}$. □

Proving Claim D.15. The proof uses Conjecture B.8 is an similar way it is used in the second part of the proof of the theorem.

Proof of Claim D.15. For $\boldsymbol{r} \in \{\mathcal{R} \cup \perp\}$, let $\mathcal{E}(\boldsymbol{r})$ be the indices of the $\perp$'s in $\boldsymbol{r}$. We assume without loss of generality that a party aborts upon getting $\perp$ as its second round random coins. For $\boldsymbol{f} \in \operatorname{Supp}(D_{\mathcal{F}})$, $d \in [h-1]$ and $b \in \{0,1\}$, let

$$\mathcal{A}_b^{\boldsymbol{f}} = \left\{\boldsymbol{r} \in \{\mathcal{R} \cup \perp\} : \Pi_d(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{E}(\boldsymbol{r})}} = b^{\left|\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{E}(\boldsymbol{r})}\right|}\right\} \tag{25}$$

By definition, for $\boldsymbol{f} \in \mathcal{T}_{d,0} \cap \mathcal{T}_{d,1}$ and $b \in \{0,1\}$, it holds that

$$\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n}\left[\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b^{\boldsymbol{f}}\right] \geq \lambda\right] \geq 1 - \delta \tag{26}$$

By Conjecture B.8, see Equation (16), for $\boldsymbol{f} \in \mathcal{T}_{d,0} \cap \mathcal{T}_{d,1}$ it holds that

$$\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\forall b \in \{0,1\} \colon \ \{\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b^{f} \neq \emptyset\right] > \delta$$

That is,

$$\Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\forall b \in \{0,1\} \quad \exists \mathcal{S}_b \in \{\mathcal{S}, \emptyset\} : \Pi_d^{\mathcal{S}_b}(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}} = b^{\left|\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}\right|}\right] > \delta \tag{27}$$

In pursuit of contradiction, assume that $\Pr\left[\mathcal{T}_{d,0} \mid \widetilde{\mathcal{T}}\right] + \Pr\left[\mathcal{T}_{d,1} \mid \widetilde{\mathcal{T}}\right] \geq 1 + \lambda/(h \cdot \Pr[\widetilde{\mathcal{T}}])$ for some $d \in [h-1]$. It follows that

$$\begin{aligned} &\Pr_{\substack{\boldsymbol{f} \leftarrow D_{\mathcal{F}} \\ \boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}}\left[\forall b \in \{0,1\} \quad \exists \mathcal{S}_b \in \{\mathcal{S}, \emptyset\} : \Pi_d^{\mathcal{S}_b}(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}} = b^{\left|\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}\right|}\right] \qquad (28) \\ &> \Pr\left[\mathcal{T}_{d,0} \cap \mathcal{T}_{d,1}\right] \cdot \delta \\ &\geq \Pr\left[\widetilde{\mathcal{T}}\right] \cdot \Pr\left[\mathcal{T}_{d,0} \cap \mathcal{T}_{d,1} \mid \widetilde{\mathcal{T}}\right] \cdot \delta \\ &\geq \Pr\left[\widetilde{\mathcal{T}}\right] \cdot \lambda/(h \cdot \Pr[\widetilde{\mathcal{T}}]) \cdot \delta \\ &= \lambda\delta/h \\ &> 8\alpha. \end{aligned}$$

The first inequality is by Equation (27), the second one by the assumption that $\Pr\left[\mathcal{T}_{d,0} \mid \widetilde{\mathcal{T}}\right] + \Pr\left[\mathcal{T}_{d,1} \mid \widetilde{\mathcal{T}}\right] \geq 1 + \lambda/(h \cdot \Pr[\widetilde{\mathcal{T}}])$, and the last one by the definition of α.
Consider the following rushing adversary:

Algorithm D.17 (A)**.**

Preinteraction.

1. *For each* $i \in [h-1]$, *estimate* $\xi_i = \Pr_{\boldsymbol{r} \leftarrow \mathcal{R}^n, \mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}\left[\forall b \in \{0,1\} \quad \exists \mathcal{S}_b \in \{\mathcal{S}, \emptyset\} : \Pi_d^{\mathcal{S}_b}(\boldsymbol{v}; (\boldsymbol{f}, \boldsymbol{r}))_{\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}} = b^{\left|\overline{\mathcal{P} \cup \mathcal{L}_d \cup \mathcal{S}_b}\right|}\right]$ *by taking* $\Theta(\log(h/\alpha)/\alpha$ *samples.*
   Let $d = \operatorname{argmax}\{\xi_i\}$.
2. *Sample a random* $\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}$ *conditioned on* $|\mathcal{S}| \leq 2\sigma n$.

Corrupt the parties in $\mathcal{P} \cup \mathcal{S} \cup \mathcal{L}_d$.

First round. *Act according to* Π_d.

Second round. *Sample* $\mathcal{S}_0, \mathcal{S}_1$ *at random from* $\{\emptyset, \mathcal{S}\}$, *and act towards some honest parties according to* $\Pi_{d,0}^{\mathcal{S}_0}$ *and towards the others according to* $\Pi_{d,1}^{\mathcal{S}_1}$.

. . . .

By Equation (28) and since $\Pr_{\mathcal{S} \leftarrow \mathbf{D}_{n,\sigma}}[\mathcal{S} \geq 2\sigma n] \leq \alpha$, the above adversary violates the agreement of Π on input $\boldsymbol{v}$ with probability larger than α, in contradiction to the assumed agreement of Π. $\square$