




On the (Im)possibility of Game-Theoretically Fair Leader Election Protocols

Ohad Klein¹ , Ilan Komargodski^{1,2} , and Chenzhi Zhu³ 

¹ Hebrew University of Jerusalem, Jerusalem, Israel

ohadkel@gmail.com, ilank@cs.huji.ac.il

² NTT Research, Sunnyvale, CA, USA

³ Paul G. Allen School of Computer Science & Engineering,

University of Washington, Seattle, WA, USA

zhucz20@cs.washington.edu

Abstract. We consider the problem of electing a leader among n parties with the guarantee that each (honest) party has a reasonable probability of being elected, even in the presence of a coalition that controls a subset of parties, trying to bias the output. This notion is called “game-theoretic fairness” because such protocols ensure that following the honest behavior is an equilibrium and also the best response for every party and coalition. In the two-party case, Blum’s commit-and-reveal protocol (where if one party aborts, then the other is declared the leader) satisfies this notion and it is also known that one-way functions are necessary. Recent works study this problem in the multi-party setting. They show that composing Blum’s 2-party protocol for $\log n$ rounds in a tournament-tree-style manner results with perfect game-theoretic fairness: each honest party has probability $\geq 1/n$ of being elected as leader, no matter how large the coalition is. Logarithmic round complexity is also shown to be necessary if we require perfect fairness against a coalition of size $n - 1$. Relaxing the above two requirements, i.e., settling for approximate game-theoretic fairness and guaranteeing fairness against only constant fraction size coalitions, it is known that there are $O(\log^* n)$ round protocols.

This leaves many open problems, in particular, whether one can go below logarithmic round complexity by relaxing only one of the strong requirements from above. We manage to resolve this problem for commit-and-reveal style protocols, showing that

- $\Omega(\log n / \log \log n)$ rounds are necessary if we settle for approximate fairness against very large (more than constant fraction) coalitions;
- $\Omega(\log n)$ rounds are necessary if we settle for perfect fairness against n^ε size coalitions (for any constant $\varepsilon > 0$).

These show that both relaxations made in prior works are necessary to go below logarithmic round complexity. Lastly, we provide several additional upper and lower bounds for the case of single-round commit-and-reveal style protocols.

1 Introduction

Suppose that Rivest, Shamir, and Adleman win yet another important award for the invention of their groundbreaking RSA crypto-system. The award committee announces that all of them are invited to the ceremony but only one of them can deliver a presentation. Since they all want to present and they all reside in different parts of the world, they need to run a leader election protocol over the internet. Of course, they are aware of Cleve's famous lower bound [5] stating that *strongly fair* protocols do not exist, i.e., in any protocol, there exists a strategy for half of the parties to bias the output. However, not all hope is lost because for their application the classical notion of fairness is overly stringent. Indeed, a recent line of works [3,8,4,17,12] observed that a relaxed notion of fairness, called *game-theoretic fairness*, in the context of leader election is often sufficient and also possible to achieve even when an arbitrary number of parties may be corrupt.

To exemplify the notion and possibility of game-theoretic fairness we recall Blum's original 2-party coin flipping protocol [2]: each party first commits to a random coin, they then open their coin, and the XOR of the two bits is used to elect the winner. If one party fails to commit or correctly open, it is eliminated and the remaining party is declared the winner. Blum's protocol satisfies game-theoretic fairness in the following sense. As long as the commitment scheme is not broken, a corrupt party cannot bias the coin to its own favor no matter how it deviates from the protocol. Note that Blum's protocol is not strongly fair since a corrupt party can indeed bias the coin, but only to the other party's advantage.

The above 2-party protocol can be generalized to handle n parties via a tournament-tree protocol, as follows. Suppose that n is a power of 2 for simplicity. We first divide the n parties into $n/2$ pairs, and each pair elects a winner using Blum's protocol. The winner survives to the next round, where we again divide the surviving $n/2$ parties into $n/4$ pairs. The protocol continues in the same manner for $\log_2 n$ rounds when a final winner is elected.⁴ At any point in the protocol, if a party fails to commit or correctly open its commitment, it is eliminated and its opponent survives to the next round.

The recent work of Chung et al. [3] proved that the above tournament-tree protocol satisfies a strong notion of game-theoretic fairness, as explained below. Suppose that the winner obtains a utility of 1 and everyone else obtains a utility of 0. As long as the commitment scheme is not broken, the tournament tree protocol guarantees that:

- No coalition of any size can *increase its own expected utility* no matter what strategy it adopts.
- No coalition of any size can *harm any individual honest player's expected utility*, no matter what strategy it adopts.

⁴ By default, throughout this paper \log stands for \log_2 .

Recent work in this space [3,8,4,17] calls the former notion cooperative-strategy-proofness (or *CSP-fairness* for short), and calls the latter notion *maximin fairness*. Philosophically, CSP-fairness guarantees that any rational, profit-seeking individual or coalition has no incentive to deviate from the honest protocol; and maximin fairness ensures that any paranoid individual who wants to maximally protect itself in the worst-case scenario has no incentive to deviate either. In summary, the honest protocol is an equilibrium and also the best response for every player and coalition. Therefore, prior works [4,3,17,8] argue that game-theoretic notions of fairness are compelling and worth investigating because (1) they are arguably more natural (albeit strictly weaker) than the classical strong fairness notion in practical applications; and (2) the game-theoretic relaxation allows us to circumvent classical impossibility results pertaining to strong fairness in the presence of majority coalitions [5].

Since we know that the tournament tree protocol satisfies game-theoretic fairness, a natural question is whether logarithmic round complexity is necessary. A protocol of [12] (following up on [3]) showed that if we settle for an approximate notion of game-theoretic fairness, then the answer is no: there are $O(\log^* n)$ -round protocols.⁵ In approximate fairness we require to satisfy the above notions of game theoretic fairness (i.e., CSP-fairness and maximin fairness) up to an ε slack. More specifically, we say that a protocol is $(1 - \varepsilon)$ -fair if every coalition’s expected utility cannot exceed $1/(n(1 - \varepsilon))$ times the size of the coalition and if any honest individual’s expected utility cannot drop below $(1 - \varepsilon)/n$. Perfect fairness holds when $(1 - \varepsilon)$ -fairness holds with $\varepsilon = 0$.

While the above works provide feasibility of round-efficient protocols for game-theoretically fair leader election, it is still widely open to characterize the minimal round complexity needed. This is a major problem left open in the works of [3,12]. Most strikingly, it is not even known if single-round commit-and-reveal style protocols exist. This seemingly simple setting with minimal interaction already turns out to be quite challenging to analyze and our work is the first to address this problem with various possibility and impossibility results.

Single-round protocols. We start by focusing on single-round “commit-and-reveal” protocols which consist of two phases: in the first phase each party commits to a value. In the second phase, each party either opens their commitment or sends a special **abort** symbol. Finally, a publicly known function is applied to the revealed values, specifying the identity of a leader. To simplify, we assume an ideal commitment scheme; this has the advantage of separating the computational issue regarding cryptography from the game-theoretic aspects of the problem. Note that this will only make our lower bounds stronger.

Before stating our main results, we want to illustrate the non-triviality of the problem by going back to the Rivest-Shamir-Adleman conundrum. As men-

⁵ In fact, their protocol enables a smooth trade-off between the round complexity and the resilience to strategic behavior, but their framework requires at least $\Omega(\log^* n)$ rounds to provide any meaningful fairness guarantee. Here $\log^* n$ denotes the minimum number of times the logarithm function must be iteratively applied to n before the result is less 1.

tioned, they can fairly decide who will deliver the presentation using a “depth-two” tournament tree (commit-and-reveal-commit-and-reveal). Can they do it using only commit-and-reveal? We answer this question by showing the following results:

1. *An upper bound:* there is a commit-and-reveal protocol achieving $(3/4)$ -fairness.
2. *A lower bound:* there is no commit-and-reveal protocol achieving $(1 - \varepsilon)$ -fairness for any $\varepsilon < 1/4$.

The upper bound is obtained via the following simple protocol: every pair runs Blum’s perfectly fair leader election protocol. A party is declared as the leader if it wins both of its tournaments. If no party won both tournaments, we simply declare party 1 as the leader. Because the pair-wise protocol is perfectly fair, any fixed party will be declared as leader with probability at least $1/4$. Thus, the protocol is $(1/4)/(1/3) = (3/4)$ -fair. The more surprising aspect of the above result is the lower bound, showing that this protocol is optimal. Our proof relies on a non-trivial application of the minimax principle. More generally, we prove the following theorem for any number of parties:

Theorem 1 (Fairness of single-round protocols; informal). *For protocols on n parties, even in the presence of a corrupted coalition of size $n - 1$:*

- *There exists $(n/2^{n-1})$ -fair single-round “commit-and-reveal” protocol.*
- *Any α -fair single-round “commit-and-reveal” protocol satisfies $\alpha \leq n/2^{n-1}$.*

Extensions. By a “grouping” argument we extend the above impossibility result to the setting where the honest set of parties consists of a constant β fraction of parties. For instance, when $\beta = 1/3$, our result shows that there is no $(8/9)$ -fair leader election protocol. See Theorem 18 for the exact statement. Lastly, we consider the low-corruption regime, i.e., when the coalition is of size say 1 or 2 and $n \geq 3$ is arbitrarily large. We show (in Theorem 25) that in this setting there are no perfectly fair leader election protocols.

Multiple-round protocols. It was shown in [3, Theorem 8.1] that $\Omega(\log n)$ rounds are required for perfectly fair leader election among n parties. When the protocol is required to be only approximately fair, the number of rounds can be reduced to $O(\log^* n)$ by [12].

This gap is due to two differences between the regimes. First, perfect fairness is more stringent, requiring $\varepsilon = 0$ in the fairness definition. Second, the $\Omega(\log n)$ lower bound implicitly assumes protection against a corrupted coalition of size $n - 1$ (which we abbreviate as $(n - 1)$ -corruption), while the $O(\log^* n)$ -round protocol assumes a constant fraction (i.e. $n - \Omega(n)$) of corrupted parties.

Therefore, there are two cases in which the round complexity is undetermined (in addition to the question of whether the $O(\log^* n)$ protocol is most round-efficient), giving rise to the following questions:

- **Question 1:** Is there a $o(\log n)$ -round protocol with guaranteed approximate fairness against coalitions of size $n - o(n)$?

- **Question 2:** Is there a $o(\log n)$ -round protocol with guaranteed perfect fairness against coalitions of size less than $n - 1$?

We answer both of the above questions by providing nearly tight lower bounds on the number of rounds in both cases. At a high level, we show that for every $\varepsilon \in (0, 1)$, perfect fairness in the presence of n^ε corrupted parties requires $\Omega(\log n)$ rounds. We proceed with a more precise statement of our results.

Approximate fairness. We show that $\Omega(\log n / \log \log n)$ rounds are necessary even in a weak $(1/n)$ -fairness requirement by extending an argument of [3]. The protocols we consider are as in [3], and are composed of a sequence of r rounds, each of which is a “commit-and-reveal” sub-protocol, as described earlier. Specifically, we prove the following theorem in Section 5.

Theorem 2 (Approximate fairness against large coalitions requires at least $\log(n) / \log \log(n)$ rounds). *A leader election protocol on n parties, having r “commit-and-reveal” rounds, in which each honest party has a chance of $1/n^2$ to be elected (i.e. $1/n$ -fairness), even in the presence of a corrupted coalition of size $n - k$, must satisfy*

$$r > \frac{\log(n) - \log(k)}{\log \log(n) + 3}.$$

We further extend this result to the case of committee election, where a small set of t parties is to be elected; see Section 5 for detail.

Perfect fairness. We also show a logarithmic lower bound on the round complexity of any perfectly fair leader election protocol in the presence of sub- $(n - 1)$ corrupted parties. Specifically, we prove the following theorem in Section 6.2.

Theorem 3 (Perfect fairness against size- k coalitions requires at least $\log k$ rounds). *A leader election protocol on n parties, having r “commit-and-reveal” rounds, which is perfectly fair in the presence of a corrupted coalition of size k , must satisfy*

$$r \geq \lceil \log(\min(n, 2k)) \rceil.$$

Organization. In Section 2, we provide a technical overview of our proofs. In Section 3, we define fairness, committee-election protocols, and prove an n -party minimax theorem. In Section 4, we give a tight bound on the fairness of single-round protocols. In Section 5, we apply this bound to bound the round-efficiency of reasonably-fair protocols. Finally, in Section 6, we lower bound the number of rounds of perfectly fair protocols.

1.1 Additional Related Work

There are several prior results on lower bounds of coin flipping protocols that imply certain impossibility results of leader election protocols. In the information-theoretical regime, Russel, Saks and Zuckerman [14] showed that for any n -party

coin flipping protocols with $r = o(\log^* n)$ rounds where each party can only send one bit per round, a coalition of a constant fraction of parties can bias the outcome. Later, Filmus et. al. [7] extended the results to protocols where each party is allowed to send arbitrary messages. In the setting where a constant fraction of parties are corrupted, since a fair n -party r -round leader election protocol implies an n -party $(r + 1)$ -round coin flipping protocol safe against a constant bias, the results imply that there is no fair n -party leader election protocol with $r = o(\log^* n)$ rounds in the information-theoretical regime. The $(\log^* n + O(1))$ -round protocol by Russell and Zuckerman [15] and Feige’s famous lightest bin protocol [6] show that the above lower bounds are tight.

A result by Berman, Haitner and Tentes [1] (improving on [11]) shows that any 2-party weak coin flipping protocol safe against any constant bias implies the existence of one-way functions. Here the security of 2-party weak coin flipping guarantees that the adversary cannot bias the outcome towards 1 by corrupting party one and cannot bias the outcome towards 0 by corrupting party two. The result implies that any fair n -party leader election protocol in the dishonest majority setting implies the existence of one-way functions, since such an n -party leader election protocol implies a 2-party weak coin flipping protocol safe against a constant bias.

We also note that there is a line of work on random selection protocols in the information-theoretical regime [9,16,10], wherein n parties want to agree on a random value sampled from a output universe of size p and the security goal is to prevent the corrupted parties from causing the output to lie in some small subset of the output universe. Although one can view a random selection protocol as a leader election protocol for $p = n$, we emphasize that their security goal is very different from our fairness notion. In particular, they do not prevent an attacker that controls $n - 1$ parties from always making sure that the output is one of the corrupted $n - 1$ parties, which is exactly the setting that we are interested in. As another evidence of the difference, Gradwohl, Vadhan and Zuckerman [10] give a $\log^*(n)$ -round random selection protocol in the dishonest majority setting without using any cryptography/ideal model commitments, while for our notion of fairness this is impossible [1] (as mentioned above).

1.2 Open Problems

One limitation of our impossibility results is that we only consider the commit-and-reveal style protocols, and it is unclear whether we can generalize our impossibility results to stronger models (e.g., only assuming one-way functions or oblivious transfer).

Another main open problem is whether we can extend our lower bounds on the number of rounds to the setting where the number of honest parties is greater than $n/\log n$. For example, when a constant fraction of parties are honest, the protocol of [12] needs $O(\log^* n)$ rounds, but we do not know whether this is optimal.

Regarding upper bounds, for the $(n - 1)$ -corruption case, we only know that there are perfectly fair protocols with $\log n$ rounds, but it is unclear whether

we can do slightly better than $\log n$ rounds for approximate fairness. Our lower bound shows that a fair protocol needs at least $\frac{\log n}{\log \log n + O(1)}$ rounds. It is interesting to see whether we can close this gap.

In the regime of perfect fairness, it is unclear whether our lower bound is tight. Even if the adversary only corrupts a single party, it is unclear whether we can construct a *perfectly fair* leader election protocol with $r < \log n$ rounds or show it is impossible. Also, for single-round protocols, we only show there is no perfect leader election protocol, but it is unclear whether it can be extended to committee election protocol. For example, it is unclear whether we can elect 2 out of 5 parties by a single round protocol with perfect fairness assuming only one party is malicious.

2 Technical Overview

In this section we describe the technical methods underlying the proofs of our main results. In Section 2.1 we explain the ideas behind the proof of the single-round setting Theorem 1, and in Section 2.2 we explain how to obtain our results in the multi-round setting, i.e., Theorems 2 and 3.

For the lower bounds of approximate fairness, we focus on the $(n - 1)$ -corruption case in the following explanations. Our results for $(n - k)$ -corruption follow by “grouping” various sets of parties together and treating them as one, as follows: Roughly, given a fair n -party protocol against $(n - k)$ -corruptions, we construct a fair n/k -party protocol against $(n/k - 1)$ -corruptions by partitioning n parties into n/k groups of size k and viewing each group as a single party. We refer to Sections 4.3 and 5.1 for details on this reduction.

2.1 Lower Bounds for Single-Round Commit-and-Reveal Protocols

Given a single-round n -party commit-and-reveal leader election protocol, we show that there exists an adversary corrupting $n - 1$ parties such that the probability that the honest party is the leader is at most $2^{-(n-1)}$. Since the protocol is commit-and-reveal, the adversary must choose the inputs for all corrupted parties before seeing the honest party’s input. After receiving the honest party’s input, the only strategy of the adversary is to let some corrupt parties abort.

The idea of our attack is to let all but one corrupted party abort. After receiving the input of the honest party, the adversary checks whether there exists a corrupted party i such that party i wins against the honest party if all corrupted parties except party i abort. Denote the event that the honest party j wins against party i as Loss_i . The intuition that this attack works is that, on average, the probability that Loss_i occurs should be at most $1/2$, and therefore, since there are $n - 1$ corrupted parties, the probability that no corrupted party wins against the honest party should be at most $2^{-(n-1)}$.

However, this simple argument does not work. The main issue is that the two events Loss_i and Loss_k for two corrupted parties i and k are not independent. In fact, they both depend on the input of the honest party j . The idea to address

this is to fix the input of the honest party in our analysis. Since Loss_i depends only on the inputs of party i and the honest party, assuming the adversary chooses the input of each corrupted party independently, the events Loss_i and Loss_k are independent given the input of the honest party x_j . Therefore, the probability that the honest party is the leader is at most $\max_x \prod_i \Pr[\text{Loss}_i|x]$, where $\Pr[\text{Loss}_i|x]$ denotes as the probability that Loss_i occurs given that x is input of the honest party.

The problem then reduces to bounding $\max_x \prod_i \Pr[\text{Loss}_i|x]$. To this end, we define a few notations for describing the adversary's strategy. We use \mathcal{S}_i to denote a (mixed) strategy for choosing the input of party i . We denote $p_{i,j}(\mathcal{S}_i, x_j)$ as the probability that Loss_i occurs under the strategy \mathcal{S}_i given that party j is the honest party and the input of party j is x_j . Then, the probability that the honest party j wins and elected as the leader is upper bounded by

$$W_j = \min_{\{\mathcal{S}_i\}_{i \in [n] \setminus \{j\}}} \max_{x_j} \prod_i p_{i,j}(\mathcal{S}_i, x_j). \quad (1)$$

Recall that the protocol is 'not fair' even if for one specific j the value W_j is too small. We will even show that the expected value of $\log(W_j)$ over uniformly random $j \sim [n]$ is small.

To bound (1), we use the minimax theorem from game theory. The minimax theorem shows that for any two parties i and j , $\min_{\mathcal{S}_i} \max_{x_j} p_{i,j}(\mathcal{S}_i, x_j) + \min_{\mathcal{S}_j} \max_{x_i} p_{j,i}(\mathcal{S}_j, x_i) = 1$. Therefore, denoting $p_{i,j} := \min_{\mathcal{S}_i} \max_{x_j} p_{i,j}(\mathcal{S}_i, x_j)$, we rewrite the minimax equation as $p_{i,j} + p_{j,i} = 1$ for all $i \neq j \in [n]$. Also, the probability that the honest party is the leader is bounded by $\prod_{i \in [n] \setminus \{j\}} p_{i,j}$.

Overall, we converted the problem to the following question: given $0 \leq p_{i,j} \leq 1$ and $p_{i,j} + p_{j,i} = 1$ for all $i \neq j \in [n]$, show that there exists j such that $\prod_{i \in [n] \setminus \{j\}} p_{i,j} \leq 2^{-(n-1)}$. To show this, we take the logarithm of both sides, which converts products to sums. Since $p_{i,j} + p_{j,i} = 1$, by Jensen's inequality, we have $\log p_{i,j} + \log p_{j,i} \leq 2 \log(p_{i,j}/2 + p_{j,i}/2) = -2$. It remains to show that there exists j such that $\sum_{i \in [n] \setminus \{j\}} \log p_{i,j} \leq -(n-1)$. For simplicity, we demonstrate the proof for $n = 3$. By summing of all pairs of $i \neq j$, we have

$$\log p_{2,1} + \log p_{3,1} + \log p_{1,2} + \log p_{3,2} + \log p_{1,3} + \log p_{2,3} \leq -6.$$

Therefore, one of the followings holds:

$$\begin{aligned} \log(W_1) &= \log p_{2,1} + \log p_{3,1} \leq -2, \\ \log(W_2) &= \log p_{1,2} + \log p_{3,2} \leq -2, \\ \log(W_3) &= \log p_{1,3} + \log p_{2,3} \leq -2. \end{aligned}$$

This proves that any one-round leader election protocol cannot be α -fair for $\alpha \geq 2^{-(n-1)}/(1/n) = n/2^{n-1}$. We refer to Section 4.2 for the full proof.

Extending to committee election. Committee election protocols are similar to leader election protocols, except that they elect a committee of t parties, instead of just one party. Each party wants to be elected with probability about t/n .

If we wish to show that single-round protocols are not fair, we cannot use the same adversary for committee election protocols, since it aborts all but two parties. This means that the honest party will always be elected once two parties are elected. The adversary is supposed to prevent this from happening.

To address this, the idea is to partition the corrupted parties into groups of size k where k is larger than the committee size. After receiving the honest party's input, the adversary picks a group and lets all other groups abort. Similarly to the leader election case, assuming that party j is the honest party and the input of j is x_j , for a set of parties $T \subset [n] \setminus \{j\}$ and a (mixed) strategy \mathcal{S}_T of parties in T , we denote $p_{T,j}(\mathcal{S}_T, x_j)$ the probability that the honest party is in the committee under the strategy \mathcal{S}_T given that all corrupted parties except those in T abort. Denote $p_{T,j} := \min_{\mathcal{S}_T} \max_{x_j} p_{T,j}(\mathcal{S}_T, x_j)$. By extending the minimax theorem to the $(k+1)$ -party case, we can show that $\sum_{j \in T'} p_{T' \setminus \{j\}, j} \leq t$, where $T' \subset [n]$ is a set of size $k+1$. Intuitively, this shows that on average $p_{T,j} \leq t/(k+1)$. Also, given party j as the honest party and a partition $\mathcal{P} = (T_1, \dots, T_{(n-1)/k})$ of the corrupted parties, the probability that the honest party is in the committee is bounded by $\prod_{T \in \mathcal{P}} p_{T,j}$. Using a similar calculation for the leader election case, we show that there exists party j and a partition \mathcal{P} such that $\sum_{T \in \mathcal{P}} \log p_{T,j} \leq (n-1)/k \log(t/(k+1))$. We refer to Section 4.2 for the full proof.

By setting $k = 2t-1$, the probability that the honest party is in the committee is bounded by $2^{-\frac{n-1}{2t-1}}$. We remark that other choices k cannot improve the bound asymptotically. In fact, our upper bound for single-round committee election protocols indicates that the lower bound is tight up to a constant factor in the exponent. Intuitively, the lower bound means that it is not possible to fairly elect a committee of size smaller than $O(n/\log n)$ in one-round, which is a useful fact used in proving the lower bounds of multi-round protocols (that we discuss next).

2.2 Extending to Multi-Round Protocols

Here, we shall focus on leader election protocols and note that similar arguments apply to committee election protocols as well. The key step is to show the following inductive argument: given an α -fair r -round n -party commit-and-reveal leader election protocol Π , there exists an α' -fair $(r-1)$ -round commit-and-reveal leader election protocol Π' for $\Omega(n/\log n)$ parties, where α' is not significantly lower than α . Intuitively, this means that at each round the number of parties can only shrink by at most a factor of $1/\log n$. Therefore, a fair n -party leader election protocol requires at least $\frac{\log n}{\log \log n + O(1)}$ rounds.

We prove such a reduction as follows. After the first round of commit-and-reveal, we observe that some parties might be “eliminated,” making the probability that these parties are elected become small or 0. We first show that the number of parties that are *not* “eliminated” is $\Omega(n/\log n)$, meaning that the number of parties after the first round does not shrink too much. We show this by viewing the first round as a single-round committee election protocol, where the elected committee is the set of parties that are *not* “eliminated.” Now, we

use our lower bound for single-round committee election protocols to conclude that the number of parties that are not “eliminated” is $\Omega(n/\log n)$. Finally, we construct Π' from Π by fixing the first-round execution and grouping all eliminated parties together with one of the remaining parties as one party.

To make the above argument formal, we need to first define the condition under which a party is eliminated formally and show that the condition implies that Π' is α' -fair for some $\alpha' > 0$. Concretely, after the first-round execution, we say a party i is eliminated if and only if there exists an adversary corrupting all but party i such that the probability that i is elected is smaller than $\alpha/n - 2/n^2$. Then, for the resulting $(r - 1)$ -round protocol, no matter which parties the adversary corrupts the probability that the honest party is elected is at least $\alpha/n - 2/n^2$, meaning that the $(r - 1)$ -round protocol is $\Omega((\alpha - 2/n)/\log n)$ -fair.

Also, we need to show that there exists a first-round execution such that the number of remaining (non-eliminated) parties is $\Omega(n/\log n)$. We prove it by contradiction. Suppose this is not true. By our lower bound of single-round committee election protocols, there exists an adversary such that the honest party is not eliminated after the first round with probability at most $1/n^2$. Therefore, by the definition of “elimination,” we can construct an adversary such that the honest party is elected as the leader with probability at most $\varepsilon/n - 1/n^2$, which contradicts the fact that Π is ε -maximin-fair. The full details are given in Section 5.

2.3 Lower Bounds for Perfectly Fair Protocols

The prior result [3] by Chung et. al. shows that any perfectly fair n -party leader election protocol against $(n - 1)$ -corruption is at least $\lceil \log n \rceil$ -round. We extend their result to protocols against k -corruption by showing that the requirement for the number of corrupted parties in the following key step of their proof can be relaxed. Concretely, their proof shows that for any perfectly fair n -party leader election protocol against $(n - 1)$ -corruption, there exists a first-round execution such that given the first-round execution, the number of parties left is at least $n/2$, where we say a party is eliminated if the probability that the party is elected is 0. We relax the condition of $(n - 1)$ -corruption in the above claim and show that for any perfectly fair n -party leader election protocol against k -corruption, there exists a first-round execution such that given the first-round execution, the number of parties left is at least $\min\{n/2, k\}$. Given the first-round execution, we can view the rest of the execution of the protocol as a protocol for $\min\{n/2, k\}$ parties by fixing the execution for all the eliminated parties arbitrarily. Intuitively, since there are k corrupted parties, the resulting protocol must be perfectly fair even if all but one party are corrupted. Since the prior result indicates that the resulting protocol needs at least $\lceil \log(\min\{n/2, k\}) \rceil$ rounds, the n -party protocol needs at least $\lceil \log(\min\{n/2, k\}) \rceil + 1$ rounds. We refer to Section 6 for details.

3 Preliminaries

Notations. We use $[n]$ to denote the set $\{1, \dots, n\}$ and $[\ell..n]$ to denote the set $\{\ell, \dots, n\}$. We use $\mathbf{x} \in \Omega^n$ to denote a vector and x_i to denote the i -th entry of \mathbf{x} . We always use $\log x$ to denote the logarithm of x to the base 2.

3.1 Commit-and-Reveal Committee Election Protocols

An (n, r, t) -commit-and-reveal committee election protocol is a $2r$ -round interactive protocol among n parties that outputs a committee of size at most t . In this context, we assume that each party has a public identity $1, 2, \dots, n$, and that the interaction is synchronous, so that the protocol proceeds in rounds. Further, we use the notion of an ideal commitment functionality \mathcal{F}_{com} , as defined in Figure 1.

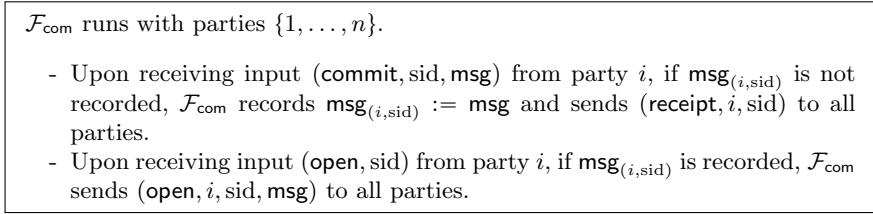


Fig. 1. The ideal commitment functionality \mathcal{F}_{com}

For each $i \in [r]$, in the $(2i - 1)$ -th round, each party j picks an element $x_j^{(i)}$ from Ω and sends $(\text{commit}, i, x_j^{(i)})$ to \mathcal{F}_{com} . W.l.o.g., in an honest execution, we assume that $x_j^{(i)}$ is sampled uniformly from Ω . In the $2i$ -th round, after receiving $(\text{receipt}, j', i)$ for each party j' , each party j sends (open, i) to \mathcal{F}_{com} . If the party aborts in either of the two rounds or does not open its commitment, we denote $x_j^{(i')} = \perp$ for $i \leq i' \leq r$. Finally, each party uses a deterministic algorithm which takes $(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)})$ as input to compute the selected committee. Since all communication relies on the functionality \mathcal{F}_{com} , which implicitly implies broadcast channels, each party receives the same view during the execution of the protocol, and thus all parties agree on the final selected committee.

For simplicity, we say the protocol is an r -round commit-and-reveal protocol. We call $\mathbf{x}^{(i)}$ the input of round i and $x_j^{(i)}$ the input of party j in round i . Formally, the commit-and-reveal committee election protocol can be represented as a function Π , indicating which parties win the election and are included in the committee (see Definition 4).

Definition 4 (Commit-and-Reveal Committee/Leader Election). *For any integers $r \geq 1$ and $1 \leq t \leq n$, an (n, r, t) -commit-and-reveal committee*

election protocol with input space Ω is a function

$$\Pi : ((\perp\} \cup \Omega)^n)^r \rightarrow (\{0, 1\})^n$$

such that for any $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)} \in (\{\perp\} \cup \Omega)^n$, $1 \leq \sum_{i=1}^n \Pi_i(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)}) \leq t$, where $\Pi_i(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)})$ denotes the i -th entry of the output of Π . In particular, an $(n, r, 1)$ -commit-and-reveal committee election protocol is an (n, r) -commit-and-reveal leader election protocol.

Remark 5. We note here that for committee election we only require the protocol to select a non-empty committee with size at most t instead of exactly t . This is because we mainly consider impossibility results in this paper, and our definition can cover a wider range of protocols, which makes our impossibility results stronger. Also, for our positive results (see Section 4.1), our committee election protocol does always select t parties.

Security. An adversary can corrupt k parties at the beginning, before the rounds begin. Since we use the ideal commitment functionality, during each round, the only strategy of the adversary is to choose the inputs of all corrupt parties independent of all honest parties' inputs (for that round) and decide, for each corrupted party, whether to abort according to the revealed inputs of the honest parties. That is, we assume the adversary is *rushing*, i.e., the adversary can decide whether to abort after observing all honest parties' revealed inputs.

Fairness. We use the same fairness definition as [12]. Maximin-fairness means that the adversary cannot decrease the probability that an honest party is in the committee by a factor of $(1 - \varepsilon)$, and is formally defined in Definition 6. Furthermore, CSP-fairness means that the adversary cannot increase the expected fraction of corrupted parties in the committee by a factor of $\frac{1}{1 - \varepsilon}$, and is formally defined in Definition 7.

Definition 6 (Maximin-Fairness). We say that an (n, r, t) -commit-and-reveal committee election protocol is $(1 - \varepsilon, k)$ -maximin-fair if for any adversary \mathcal{A} that corrupts a set $S \subseteq [n]$ of parties of size k , and for any $i \in [n] \setminus S$,

$$\Pr[i \text{ is in the committee}] \geq \frac{(1 - \varepsilon)t}{n},$$

where the probability is taken over the randomness of \mathcal{A} and all honest parties' inputs $\{x_j^{(\ell)}\}_{j \in [n] \setminus S, \ell \in [r]}$ with $x_j^{(\ell)}$ sampled uniformly from Ω .

Definition 7 (CSP-Fairness). We say that an (n, r, t) -committee election protocol is $(1 - \varepsilon, k)$ -CSP-fair if for any adversary \mathcal{A} that corrupts a set $S \subseteq [n]$ of parties of size k ,

$$\mathbb{E}[\text{the fraction of corrupted parties in the committee}] \leq \frac{k}{n(1 - \varepsilon)},$$

where the expectation is taken over the randomness of \mathcal{A} and all honest parties' inputs $\{x_j^{(\ell)}\}_{j \in [n] \setminus S, \ell \in [r]}$ with $x_j^{(\ell)}$ sampled uniformly from Ω .

Moreover, we say a scheme is $(1 - \varepsilon, k)$ -fair if the scheme is both $(1 - \varepsilon, k)$ -maximin-fair and $(1 - \varepsilon, k)$ -CSP-fair. We say a scheme is perfectly fair against k -corruption if and only if the scheme is $(1, k)$ -fair.

3.2 Minimax Theorem

We first recall the minimax theorem from game theory, which was first proved in [13]. Then, we show an n -variable extension of the theorem, which is used in our proofs of lower bounds for single-round protocols. For any n -variable function $f : \Omega^n \rightarrow \mathbf{R}$, a (mixed) strategy for a set $S \subseteq [n]$ (of players) is a probability distribution over all inputs $\{x_i \in \Omega\}_{i \in S}$. Such a strategy can be regarded as a function $\mathcal{S} : \Omega^{|S|} \rightarrow [0, 1]$ such that $\sum_{\mathbf{x} \in \Omega^{|S|}} \mathcal{S}(\mathbf{x}) = 1$. Given two strategies $\mathcal{S}_1, \mathcal{S}_2$ where \mathcal{S}_1 is for $S \subseteq [n]$ and \mathcal{S}_2 is for $[n] \setminus S$, we denote

$$f(\mathcal{S}_1, \{x_j\}_{j \in [n] \setminus S}) := \sum_{\{x_i\}_{i \in S} \in \Omega^{|S|}} \mathcal{S}_1(\{x_i\}_{i \in S}) f(x_1, \dots, x_n)$$

and

$$f(\mathcal{S}_1, \mathcal{S}_2) := \sum_{\mathbf{x} \in \Omega^n} \mathcal{S}_1(\{x_i\}_{i \in S}) \mathcal{S}_2(\{x_j\}_{j \in [n] \setminus S}) f(x_1, \dots, x_n).$$

Theorem 8 (Minimax Theorem [13]). *For any 2-variable function $f : \Omega^2 \rightarrow \mathbf{R}$, we have*

$$\max_{\mathcal{S}_1} \min_{\mathcal{S}_2} f(\mathcal{S}_1, \mathcal{S}_2) = \min_{\mathcal{S}_2} \max_{\mathcal{S}_1} f(\mathcal{S}_1, \mathcal{S}_2),$$

where \mathcal{S}_1 denotes a strategy for the first input and \mathcal{S}_2 denotes a strategy for the second input.

Using the above theorem, we deduce the following lemma, which can be viewed as an n -variable extension of the original minimax theorem.

Lemma 9 (n -Party Minimax). *For any $k \in \mathbf{R}$, and any n -variable functions $f_1, \dots, f_n : \Omega^n \rightarrow \mathbf{R}$ such that $\sum_{i \in [n]} f_i(\mathbf{x}) \leq k$ for any $\mathbf{x} \in \Omega^n$, we have*

$$\sum_{i \in [n]} \min_{\mathcal{S}_i} \max_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) \leq k,$$

where \mathcal{S}_i denotes a strategy for $[n] \setminus \{i\}$ and \mathcal{S}_i denotes a strategy for $\{i\}$.

Remark 10. In order to see that Lemma 9 extends Theorem 8, we can apply the former twice with $(f_1, f_2, k) = (f, -f, 0)$ and with $(f_1, f_2, k) = (-f, f, 0)$ respectively.

Proof. By viewing f_i as a two-variable function and applying Theorem 8, we have

$$\min_{\mathcal{S}_i} \max_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) = \max_{\mathcal{S}_i} \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) .$$

For each $i \in [n - 1]$, there exists $\mathcal{S}_i^{(0)}$ such that

$$\max_{\mathcal{S}_i} \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) = \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i^{(0)}) .$$

Then, for each $i \in [n - 1]$,

$$\min_{\mathcal{S}_n} f_i(\mathcal{S}_1^{(0)}, \dots, \mathcal{S}_{n-1}^{(0)}, \mathcal{S}_n) \geq \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i^{(0)}) = \max_{\mathcal{S}_i} \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) .$$

Therefore,

$$\begin{aligned} \max_{\mathcal{S}_{\hat{n}}} \min_{\mathcal{S}_n} \sum_{i \in [n-1]} f_i(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) &\geq \min_{\mathcal{S}_n} \sum_{i \in [n-1]} f_i(\mathcal{S}_1^{(0)}, \dots, \mathcal{S}_{n-1}^{(0)}, \mathcal{S}_n) \\ &\geq \sum_{i \in [n-1]} \min_{\mathcal{S}_n} f_i(\mathcal{S}_1^{(0)}, \dots, \mathcal{S}_{n-1}^{(0)}, \mathcal{S}_n) \\ &\geq \sum_{i \in [n-1]} \max_{\mathcal{S}_i} \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) . \end{aligned} \quad (2)$$

Thus,

$$\begin{aligned} \sum_{i \in [n]} \min_{\mathcal{S}_i} \max_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) &= \min_{\mathcal{S}_{\hat{n}}} \max_{\mathcal{S}_n} f_n(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) + \sum_{i \in [n-1]} \max_{\mathcal{S}_i} \min_{\mathcal{S}_i} f_i(\mathcal{S}_i, \mathcal{S}_i) \\ &\leq \min_{\mathcal{S}_{\hat{n}}} \max_{\mathcal{S}_n} \left(k - \sum_{i \in [n-1]} f_i(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) \right) + \max_{\mathcal{S}_{\hat{n}}} \min_{\mathcal{S}_n} \sum_{i \in [n-1]} f_i(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) \\ &= k - \left(\max_{\mathcal{S}_{\hat{n}}} \min_{\mathcal{S}_n} \sum_{i \in [n-1]} f_i(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) \right) + \max_{\mathcal{S}_{\hat{n}}} \min_{\mathcal{S}_n} \sum_{i \in [n-1]} f_i(\mathcal{S}_{\hat{n}}, \mathcal{S}_n) \\ &= k , \end{aligned}$$

where the first equality is due to the minimax theorem, the first inequality is due to Equation (2), and the next equality is due to the fact that $\min_x -f(x) = -\max_x f(x)$.

4 Upper and Lower Bounds of Single-Round Protocols

In this section, we first show a single-round n -party commit-and-reveal leader election protocol that is $(n/2^{n-1}, n - 1)$ -fair. Then, we show that the protocol is optimal by proving a tight lower bound for the $(n - 1)$ -corruption case. Finally, we extend the results to a general corruption setting .

We extend both the upper and lower bounds to committee election protocols. The bounds we get are tight up to a constant factor in the exponent for the $(n - 1)$ -corruption case. These bounds are used in the next section when we extend our lower bounds to multi-round protocols.

The parties are divided into t groups with size at most $\lceil n/t \rceil$. Within each group, we denote the parties as $\{1, \dots, \ell\}$. The input of each party i is $x_i \in \{0, 1\}^\ell \times [\ell]$. Given all parties' inputs (x_1, \dots, x_ℓ) , at most one party in $\{1, \dots, \ell\}$ is selected in the committee as follows.

- For each pair $1 \leq i < j \leq \ell$, if $x_i[j] \oplus x_j[i] = 1$, we say party i wins against party j . Otherwise, we say party j wins against party i . If one of the parties aborts, i.e., $x_i = \perp$ or $x_j = \perp$, then the other party wins against the party that aborts.
- Party i is selected if party i wins against all other parties in the group.
- If such i does not exist, the first party is selected.

Fig. 2. The single-round commit-and-reveal committee election protocol Π_{opt} .

4.1 Optimal Single-Round Leader Election

The protocol works as follows. We let each pair of parties run a 2-party tournament. I.e., each party first commits to a random bit, which is then revealed in the second round, and the winner of the tournament is indicated by the XOR of the two revealed bits. If one of the two parties aborts, the other party is the winner of the tournament. Finally, if there exists a party that wins all its tournaments, then the party is selected as the leader (note that the winner is unique). Otherwise, we select an arbitrary party.

Remark 11. We note that we can easily make the protocol perfectly fair in honest executions by letting a random party be selected when there is no party that won all its tournaments. More concretely, this can be done by letting party 1 additionally sample a random index $i \in [n]$ and put it in the input. If there is no party that won all its tournaments, party i will be selected as the leader. We will see that this change will not affect our analysis of fairness, and we only show a version without perfect fairness in honest executions for simplicity of presenting the protocol.

Since the probability that any honest party wins each tournament is at least $1/2$, the probability of any honest party to be selected as the leader is at least $1/2^{n-1}$, no matter how the corrupted parties behave. This implies that the protocol is $(n/2^{n-1}, n-1)$ -fair. The above protocol can be extended to select a committee of size t , by dividing the parties into t groups with sizes at most $\lceil n/t \rceil$, and electing a leader inside each group using the previous method. Similarly, the probability of any honest party to be selected is at least $2^{-(\lceil n/t \rceil - 1)}$. This protocol is detailed in Figure 2, and is denoted by Π_{opt} .

Theorem 12. *For any $n \geq 2$ and $1 \leq t \leq n/2$, there exists a $(n, 1, t)$ -commit-and-reveal committee election protocol that is $(2^{-(\lceil n/t \rceil - 1)} \frac{n}{t}, n-1)$ -fair. In particular, for $t = 1$, there exists a $(n, 1)$ -commit-and-reveal leader election protocol that is $(2^{-(n-1)} n, n-1)$ -fair.*

Proof. We show that Π_{opt} is $(2^{-\lfloor n/t \rfloor - 1} \frac{n}{t}, n-1)$ -fair. Let \mathcal{A} be an adversary that corrupts $n-1$ parties. For any honest party, no matter how \mathcal{A} behaves, the probability that it wins against another party in its group is at least $1/2$. Therefore, the probability that the honest party is in the committee is at least $2^{-\lfloor n/t \rfloor - 1}$, which implies that Π_{opt} is $(\alpha, n-1)$ -maximin-fair, where $\alpha := 2^{-\lfloor n/t \rfloor - 1} \frac{n}{t}$. This also implies that the expected fraction of corrupted parties in the committee is at most $\frac{t-2^{-\lfloor n/t \rfloor - 1}}{t}$, which means Π_{opt} is $(\frac{n-1}{n-\alpha}, n-1)$ -CSP-fair. Since $\alpha \leq 1$ and $\frac{n-1}{n-\alpha} \geq \frac{1}{2-\alpha} \geq \alpha$, Π_{opt} is $(\alpha, n-1)$ -fair. \square

4.2 Lower Bound for $(n-1)$ -Corruption

We show the above leader election protocol has the best possible fairness guarantee by showing the following theorem.

Theorem 13 (Single-Round, $(n-1)$ -Corruption). *For any integers $1 \leq t \leq n/2$, there is no $(n, 1, t)$ -commit-and-reveal committee election protocol that is $(\alpha, n-1)$ -fair for $\alpha > 2^{-\lfloor \frac{n-1}{2t-1} \rfloor} \frac{n}{t}$.*

Remark 14. Note that in the $t = 1$ case, which corresponds to leader election, Theorem 13 shows that the protocol Π_{opt} is optimally fair when exposed to $n-1$ corruptions.

Remark 15. In the proof, we show a slightly stronger result that there is no $(\alpha, n-1)$ -maximin-fair protocol for $\alpha > 2^{-\lfloor \frac{n-1}{2t-1} \rfloor} \frac{n}{t}$.

Proof. Let Π be an $(n, 1, t)$ -commit-and-reveal committee election protocol. For any set $T \subseteq [n]$, suppose all parties not in T abort. Denote Π^T as the protocol Π given all parties not in T abort, i.e., $\Pi^T(\{x_i\}_{i \in T}) := \Pi(\{x'_i\}_{i \in [n]})$, where $x'_i = x_i$ if $i \in T$ and $x'_i = \perp$ otherwise.

For each $i \in T$, there exists a strategy $\mathcal{S}_{T,i}$ for the players $T \setminus \{i\}$ that minimizes $\max_{x_i \in \Omega} \Pi_i^T(\mathcal{S}_{T,i}, x_i)$, where $\Pi_i^T(\mathcal{S}_{T,i}, x_i)$ is defined according to Section 3.2. By Lemma 9, we have that

$$\sum_{i \in T} \max_{x_i \in \Omega} \Pi_i^T(\mathcal{S}_{T,i}, x_i) \leq t. \quad (3)$$

Denote $p_{T,i} := \max_{x_i \in \Omega} \Pi_i^T(\mathcal{S}_{T,i}, x_i)$, which is the maximal probability that party i is in the committee under $\mathcal{S}_{T,i}$. We let $t \leq k \leq n$ be an arbitrary integer and denote $\ell := \lfloor (n-1)/k \rfloor$. To construct an adversary \mathcal{A} , we pick an index $i \in [n]$ as the honest party (the party \mathcal{A} does not corrupt) and pick a partition $P = (T_1, \dots, T_\ell)$ of $[n] \setminus \{i\}$ such that one of groups is of size $k' = n-1 - k(\ell-1)$ and all the other groups are of size k . We note here that $k' \geq k$. Denote \mathcal{P}_i as the set of all such partitions.

For each T_j , \mathcal{A} uses the strategy $\mathcal{S}_{T_j \cup \{i\}, i}$ to sample the inputs for the parties in T_j . After \mathcal{A} sees the input of party i , it picks a T_j (if any) such that party i

is not in the committee if all corrupted parties not in T_j aborts. Otherwise, \mathcal{A} does nothing. Thus, the probability that party i is in the committee is at most

$$\begin{aligned}
& \Pr_{x_i \sim \Omega, \{x'_i\}_{i' \in T_j} \sim \mathcal{S}_{T_j \cup \{i\}, i}} \left[\bigwedge_{j \in [\ell]} \Pi_i^{T_j \cup \{i\}}(\{x'_i\}_{i' \in T_j \cup \{i\}}) = 1 \right] \\
& \leq \max_{x_i \in \Omega} \Pr_{\{x'_i\}_{i' \in T_j} \sim \mathcal{S}_{T_j \cup \{i\}, i}} \left[\bigwedge_{j \in [\ell]} \Pi_i^{T_j \cup \{i\}}(\{x'_i\}_{i' \in T_j \cup \{i\}}) = 1 \right] \\
& = \max_{x_i \in \Omega} \prod_{j \in [\ell]} \Pr_{\{x'_i\}_{i' \in T_j} \sim \mathcal{S}_{T_j \cup \{i\}, i}} \left[\Pi_i^{T_j \cup \{i\}}(\{x'_i\}_{i' \in T_j \cup \{i\}}) = 1 \right] \\
& \leq \prod_{j \in [\ell]} \max_{x_i \in \Omega} \Pi_i^{T_j \cup \{i\}}(\mathcal{S}_{T_j \cup \{i\}, i}, x_i) \\
& = \prod_{j \in [\ell]} p_{T_j \cup \{i\}, i},
\end{aligned}$$

where the probability is taken over uniform choice of x_i from Ω and the randomness used by $\mathcal{S}_{T_j \cup \{i\}}$. Also, note that the second equality is due to the fact that the event $\Pi_i^{T_j \cup \{i\}}(\mathcal{S}_{T_j \cup \{i\}, i}, x_i) = 1$ and $\Pi_i^{T_{j'} \cup \{i\}}(\mathcal{S}_{T_{j'} \cup \{i\}, i}, x_i) = 1$ are independent for $j' \neq j$ given a fixed x_i .

It is left to show there exists an index $i \in [n]$ and a partition $P \in \mathcal{P}_i$ such that the above probability is small. By summing over all possible i and partitions,

$$\begin{aligned}
& \sum_{i \in [n]} \sum_{P \in \mathcal{P}_i} \log \left(\prod_{T \in P} p_{T \cup \{i\}, i} \right) = \sum_{i \in [n]} \sum_{P \in \mathcal{P}_i} \sum_{T \in P} \log(p_{T \cup \{i\}, i}) \\
& = \sum_{\substack{T' \subseteq [n] \\ |T'| \in \{k+1, k'+1\}}} \sum_{i \in T'} \sum_{(T' \setminus \{i\}) \in P \in \mathcal{P}_i} \log(p_{T', i}) \\
& = \sum_{\substack{T' \subseteq [n] \\ |T'| \in \{k+1, k'+1\}}} \sum_{P \in \mathcal{P}_{T'}} \sum_{i \in T'} \log(p_{T', i}) \\
& \leq \sum_{\substack{T' \subseteq [n] \\ |T'| \in \{k+1, k'+1\}}} \sum_{P \in \mathcal{P}_{T'}} |T'| \log(t/|T'|) \\
& = \frac{n!}{(k'+1)!(k!)^{\ell-1}(\ell-1)!} (k'+1) \log(t/(k'+1)) \\
& \quad + \frac{n!}{(k+1)!(k!)^{\ell-2}(k')(\ell-2)!} (k+1) \log(t/(k+1)) \\
& = \frac{n!}{(k!)^{\ell-1}k'!(\ell-1)!} (\log(t/(k'+1)) + (\ell-1) \log(t/(k+1))) \\
& \leq \frac{n!}{(k!)^{\ell-1}k'!(\ell-1)!} \ell \log(t/(k+1)),
\end{aligned}$$

where $\mathcal{P}_{T'}$ denotes the set of all partitions of $[n] \setminus T'$ of the form $(T_1, \dots, T_{\ell-1})$ such that, in case $|T'| = k' + 1$, each group is of size k ; in case of $|T'| = k + 1$, one of groups is of size k' and all the other groups are of size k . Also, note that the first inequality is due to Equation (3) and Jensen's inequality. Since

$$\sum_{i \in [n]} \sum_{P \in \mathcal{P}_i} 1 = \frac{n!}{(k!)^{\ell-1} k'! (\ell-1)!},$$

there exists $i \in [n]$ and $P \in \mathcal{P}_i$ such that $\log(\prod_{T \in P} p_{T \cup \{i, i\}}) \leq \ell \log(t/(k+1)) = \lfloor \frac{n-1}{k} \rfloor \log(t/(k+1))$. By setting $k = 2t-1$, we get $\log(\prod_{T \in P} p_{T \cup \{i, i\}}) \leq -\lfloor \frac{n-1}{2t-1} \rfloor$, which concludes the proof. \square

4.3 Lower Bounds for $(n - k)$ -Corruption

For any $(n, 1, t)$ -commit-and-reveal committee election protocol Π that is $(\alpha \frac{n}{t}, n-k)$ -maximin-fair, we can construct a $(n/k, 1, t)$ -commit-and-reveal committee election protocol from Π by partitioning n parties into n/k groups of size k and viewing each group as a single party. Each group is in the committee if and only if one of the party in the group is in the committee. We can show that the new protocol is $(\alpha \frac{n}{kt}, n/k - 1)$ -maximin fair.

Also, for any $(n, 1, t)$ -commit-and-reveal committee election protocol Π that is $(\frac{n-k}{n\alpha}, n-k)$ -CSP fair, i.e, for any adversary that corrupts at most $n-k$ parties, the expected fraction of corrupted parties in the committee is at most α , we can construct an $(n/k, r, t)$ -commit-and-reveal committee election protocol Π that is $(\alpha n/k, n/k - 1)$ -CSP fair from Π in the same way as the above.

Combining the above two arguments, we have the following lemma.

Lemma 16. *If there exists a (n, r, t) -commit-and-reveal committee election protocol Π that is $(\alpha, n - k)$ -fair, then there exists a $(n/k, r, t)$ -commit-and-reveal committee election protocol that is*

$$\left(\max \left\{ \frac{\alpha}{k}, \left(1 - \frac{n-k}{\alpha n} \right) \frac{n}{tk} \right\}, n/k - 1 \right) \text{-maximin fair.}$$

Remark 17. Here we only consider the case k divides n for simplicity of presenting the results as the bound would not change asymptotically for the case k does not divide n . If k does not divide n , similarly to the proof of Theorem 13, we can divide n parties into $\ell = \lfloor n/k \rfloor$ groups with $\ell - 1$ groups of size k and the last group of size $k' = n - k(\ell - 1) \geq k$, and get a $(\lfloor n/k \rfloor, r, t)$ committee election protocol Π' from a (n, r, t) committee election protocol Π . The rest of proof goes through since corrupting $\ell - 1$ parties in Π corresponds to corrupting at most $n - k$ parties in Π . The final bound on maximin fairness changes to $\max \{ \alpha \lfloor n/k \rfloor / n, (1 - (n - k)/(\alpha n)) \cdot (\lfloor n/k \rfloor / t) \}$, which is asymptotically the same as the bound in the above lemma.

Proof. For a (n, r, t) -commit-and-reveal committee election protocol Π that is $(\alpha, n - k)$ -fair, we construct a $(n/k, r, t)$ -commit-and-reveal committee election

protocol Π' from Π by partitioning n parties into n/k groups $T_1, \dots, T_{n/k}$ of size k and letting each party i in Π' simulate the behaviors of parties in T_i such that party i is selected in Π' if and only if one of parties in T_i is selected in Π .

Consider an adversary \mathcal{A} against Π' that corrupts $n/k - 1$ parties. Denote the honest party corresponding to the group T_i . We can view \mathcal{A} as an adversary \mathcal{A}' against Π that corrupts all parties not in T_i , and the number of corrupted party is $n - k$. Since Π is $(\alpha, n - k)$ -fair, it holds that (1) the probability that any honest party is selected is at least $\alpha \frac{k}{n}$ and (2) the expected fraction of corrupted parties in the committee is at most $\frac{(n-k)}{n\alpha}$.

Since T_i is selected in Π' if one of the honest parties is selected in Π , by (1), T_i is selected with probability at least $\alpha \frac{k}{n}$, which means Π' is $(\alpha/k, n/k - 1)$ -maximin fair. If T_i is not selected, then the fraction of corrupted parties in the committee is 1. By (2), it holds that $1 - \Pr[T_i \text{ is selected}] \leq \frac{(n-k)}{n\alpha}$. Therefore, the probability that T_i is selected is at least $(1 - (n-k)/(n\alpha))$, which means Π' is $((1 - (n-k)/(n\alpha))n/(tk), n/k - 1)$ -maximin fair. Therefore, we can conclude the lemma. \square

By Theorem 13 and Remark 15, we know there is no $(n/k, 1, t)$ -commit-and-reveal committee election protocol that is $(\beta, n/k - 1)$ -maximin-fair for $\beta > 2^{-\lfloor \frac{n/k-1}{2t-1} \rfloor} \frac{n}{kt}$. Therefore, by Lemma 16, we have the following theorem.

Theorem 18. *For any integers $1 \leq t \leq k \leq n/2$, there is no $(n, 1, t)$ -commit-and-reveal committee election protocol that is $(\alpha, n - k)$ -fair for*

$$\alpha > \min \left\{ 2^{-\frac{n-k}{k(2t-1)}} \frac{n}{t}, \frac{n-k}{n \left(1 - 2^{-\frac{n-k}{k(2t-1)}} \right)} \right\}.$$

In particular, for leader election protocols, there is no single-round n -party leader election protocol that is $(\alpha, n - k)$ -fair for $\alpha > \min \left\{ 2^{-\frac{n-k}{k}} n, \frac{n-k}{n \left(1 - 2^{-\frac{n-k}{k}} \right)} \right\}$.

From the above theorem, for $k = \beta n$ where $0 < \beta < 1/2$ is a constant, there is no $(n, 1)$ -commit-and-reveal leader election protocol that is $(\alpha, n(1 - \beta))$ -fair for $\alpha < \frac{1-\beta}{1-2^{-\frac{1-\beta}{\beta}}}$. For $k \leq \frac{n}{4 \log n}$, there is no $(n, 1)$ -commit-and-reveal leader election protocol that is $(1/n, n - k)$ -fair.

5 Lower Bounds for Multiple Rounds

We extend the lower bounds for single-round commit-and-reveal protocols to multi-round commit-and-reveal protocols for the $(n - 1)$ -corruption case, which is formally stated in Theorem 19. In particular, we show that there is no r -round leader election protocol that achieves constant-fairness against $(n - 1)$ -corruption for $r \leq \frac{\log n}{\log \log n + 3}$, which is implied by Corollary 20 below.

Theorem 19. For any $0 < \delta < 1$, any integer $r, t \geq 1$, and any integer $n \geq t(2 \lceil \log 1/\delta \rceil)^r$, there is no (n, r, t) -commit-and-reveal committee election protocol that is $(\alpha, n-1)$ -maximin-fair for $\alpha > r\delta n/t$.

For any $n \geq 1$, if we set $\delta = 1/n^3$, for any $r \leq \frac{\log(n/t)}{\log(2 \lceil \log n^3 \rceil)} \leq \frac{\log n - \log t}{\log \log n + 3}$, by applying the above theorem, we get the following corollary.

Corollary 20. For any integer $1 \leq t \leq n$, any integer $r \leq \frac{\log n - \log t}{\log \log n + 3}$, there is no (n, r, t) -commit-and-reveal committee election protocol that is $(\frac{1}{nt}, n-1)$ -maximin-fair.

To prove Theorem 19, the key tool is the following inductive argument. Roughly, it shows that a maximin-fair (n, r, t) -commit-and-reveal protocol implies either a maximin-fair $(n, 1, n')$ -commit-and-reveal protocol or a maximin-fair $(n', r-1, t)$ -commit-and-reveal protocol.

Lemma 21. For any integers $1 \leq t \leq n'$ and $n \geq 2n'$, any integer $r \geq 1$, and $0 < \alpha' < \alpha$, if there exists an (n, r, t) -commit-and-reveal committee election protocol that is $(\alpha n/t, n-1)$ -maximin-fair, there exists either an $(n', r-1, t)$ -commit-and-reveal committee election protocol that is $((\alpha - \alpha')n'/t, n'-1)$ -maximin-fair or an $(n, 1, n')$ -commit-and-reveal committee election protocol that is $(\alpha' n/n', n-1)$ -maximin-fair.

We use Lemma 21 through the following corollary. Intuitively, it shows that a maximin-fair (n, r, t) -commit-and-reveal protocol implies a fair $(n', r-1, t)$ -commit-and-reveal protocol for $n' = O(n/\log n)$.

Corollary 22. For any integers $1 \leq t \leq n'$ and $n \geq 2n'$, any integer $r \geq 1$, and $0 < \alpha$, if there exists a (n, r, t) -commit-and-reveal committee election protocol that is $(\alpha n/t, n-1)$ -maximin-fair, there exists an $(n', r-1, t)$ -commit-and-reveal committee election protocol that is $((\alpha - 2^{-\lfloor \frac{n-1}{2n'-1} \rfloor})n'/t, n'-1)$ -maximin-fair.

To prove Corollary 22 we note that Theorem 13 implies that there is no $(n, 1, n')$ -commit-and-reveal protocol that is $(2^{-\lfloor \frac{n-1}{2n'-1} \rfloor} \frac{n}{n'}, n-1)$ -maximin-fair. Hence, among the two options in Lemma 21, only the first is eligible. This immediately implies Corollary 22.

We now show how to prove Theorem 19 using Corollary 22.

Proof (Theorem 19). For $r = 1$, since $n \geq 2t \lceil \log(1/\delta) \rceil$ implies $2^{-\lfloor \frac{n-1}{2t-1} \rfloor} \leq 2^{-\lfloor \frac{n}{2t} \rfloor} \leq 2^{-\lceil \log(1/\delta) \rceil} \leq \delta$, the theorem follows from Theorem 13. For $r > 1$, suppose the theorem holds for $(r-1)$ -round protocols. For any $t \geq 1$ and $n \geq t(2 \lceil \log 1/\delta \rceil)^r$, assume there exists an (n, r, t) -commit-and-reveal protocol that is $(\alpha, n-1)$ -maximin-fair for $\alpha < r\delta n/t$. Let $n' = n/(2 \lceil \log 1/\delta \rceil)$. Since $2^{-\lfloor \frac{n-1}{2n'-1} \rfloor} \leq \delta$, by Corollary 22, there exists an $(n', r-1, t)$ -commit-and-reveal protocol that is $(\alpha', n'-1)$ -maximin-fair, where $\alpha' = \alpha - \delta n/t$. Since $\alpha' < (r-1)\delta n'/t$ and $n' = n/(2 \lceil \log 1/\delta \rceil) \geq t(2 \lceil \log 1/\delta \rceil)^{r-1}$, it contradicts with the assumption that the theorem holds for $(r-1)$ -round protocols. Therefore, we conclude the theorem by induction. \square

Finally, we show how to prove Lemma 21. The key idea of the proof is to consider a fixed first-round input. For an (n, r, t) -committee election protocol that is $(\alpha n/t, n-1)$ -maximin-fair, by fixing a first-round input $\mathbf{x} \in \Omega^n$, we can view it as an $(n, r-1, t)$ -committee election protocol. Then, we look into the probability p_i that each party i is in the committee if the adversary corrupts all parties but i and acts optimally. If, for any \mathbf{x} , the number of $i \in [n]$ such that $p_i \geq \alpha - \alpha'$ is more than n' , we can construct an $(n', r-1, t)$ -committee election protocol that is $((\alpha - \alpha')n'/t, n'-1)$ -maximin-fair. Otherwise, if for all \mathbf{x} , at most n' of them satisfy $p_i \geq \alpha - \alpha'$, then we can construct an $(n, 1, n')$ -committee election protocol such that given \mathbf{x} , party i is in the committee if and only if $p_i \geq \alpha - \alpha'$ and we can show this protocol is $(\alpha'n/t, n-1)$ -maximin-fair.

Proof (Lemma 21). Let Π be an (n, r, t) -commit-and-reveal committee election protocol that is $(\alpha n/t, n-1)$ -maximin-fair. Suppose there is no $(n', r-1, t)$ -committee election protocol that is $((\alpha - \alpha')n'/t, n'-1)$ -maximin-fair and no $(n, 1, n')$ -commit-and-reveal committee election protocol that is $(\alpha'n/n', n-1)$ -maximin-fair. We just need to show that there is an adversary \mathcal{A} against Π corrupting $n-1$ parties such that the probability that the honest party is in the committee is less than α . For any first-round input $\mathbf{x} \in (\{\perp\} \cup \Omega)^n$, let $T_{\mathbf{x}} := \{i \mid x_i \neq \perp\}$ and denote $\Pi^{\mathbf{x}}(\cdot) := \Pi(\mathbf{x}, \cdot)$, which is an $(n, r-1, t)$ -committee election protocol. Denote $p_{\mathbf{x}, i}$ as the minimal probability that party i is in the committee over all adversaries for $\Pi^{\mathbf{x}}$ that corrupts all parties but i . Denote $S_{\mathbf{x}} := \{i \in T_{\mathbf{x}} \mid p_{\mathbf{x}, i} \geq \alpha - \alpha'\}$.

We first show that $|S_{\mathbf{x}}| \leq n'$ for all \mathbf{x} . Suppose $|S_{\mathbf{x}}| > n'$. We construct an $(n', r-1, t)$ protocol Π' from $\Pi^{\mathbf{x}}$ as follows. We first pick an arbitrary set S' of party of size $|S_{\mathbf{x}}| - n' + 1$ from $S_{\mathbf{x}}$ and then let Π' be the same as $\Pi^{\mathbf{x}}$ except we let a single party (denoted as party i^*) simulate the behaviors of parties in $S' \cup ([n] \setminus S_{\mathbf{x}})$, while the rest of parties (i.e., parties in $S_{\mathbf{x}} \setminus S'$) acts the same as before. Party i^* is selected in Π' if and only if one of parties in the set corresponding to i^* is selected in $\Pi^{\mathbf{x}}$. Then, party i^* would be selected with probability at least $p_{\mathbf{x}, j}$ for any $j \in S'$ even if all other parties are corrupted. Also, for party each $j \in S_{\mathbf{x}} \setminus S'$, $p_{\mathbf{x}, j}$ is exactly the probability that party j is guaranteed to be elected in Π' , given that j is honest and all other $n'-1$ parties are corrupted. Therefore, each honest party among the n' players wins with probability at least $\alpha - \alpha'$. Thus, Π' is $((\alpha - \alpha')n'/t, n'-1)$ -maximin-fair, which contradict the impossibility assumption of such protocols.

We continue by describing the adversary \mathcal{A} against the original protocol Π . Consider an $(n, 1, n')$ -committee election protocol Γ defined using $S_{\mathbf{x}}$ as follows. For any input \mathbf{x} , party i is elected to be in the committee if and only if $i \in S_{\mathbf{x}}$, i.e., $\Gamma_i(\mathbf{x}) := 1\{i \in S_{\mathbf{x}}\}$. By our assumption, there is no $(n, 1, n')$ -committee election protocol that is $(\alpha'n/n', n-1)$ -maximin-fair. Therefore, there exists an adversary \mathcal{B} against Γ corrupting $n-1$ parties such that the probability of the honest party to be in the committee is at most α' . We now construct \mathcal{A} using \mathcal{B} . In the first-round, \mathcal{A} behaves exactly the same as \mathcal{B} . After the first-round, \mathcal{A} uses the best strategy for the rest of the execution. Let party i be the honest party. After the first round, if i is not in $S_{\mathbf{x}}$, where \mathbf{x} denotes the first-round message,

we know the probability that i is in the committee is at most $p_{\mathbf{x},i} < \alpha - \alpha'$. By the definition of \mathcal{B} , we have that the probability of $i \in S_{\mathbf{x}}$ is less than α' . Therefore, the probability that party i is in the committee is less than α . This concludes the proof. \square

5.1 Lower Bounds for $(n - k)$ -Corruption

By Lemma 16, if there exists a (n, r, t) -commit-and-reveal committee election protocol Π that is $(\alpha, n - k)$ -fair, then there exists a $(n/k, r, t)$ -commit-and-reveal committee election protocol that is $(\alpha/k, n/k - 1)$ -maximin-fair. Therefore, by Theorem 19, we have the following corollary.

Corollary 23. *For any $0 < \delta < 1$, any integer $r, t, k \geq 1$, and any integer $n \geq tk(2 \lceil \log 1/\delta \rceil)^r$, there is no (n, r, t) -commit-and-reveal committee election protocol that is $(\alpha, n - k)$ -maximin-fair for $\alpha > r\delta n/t$.*

For any constant $n \geq 1$, if we set $\delta = 1/n^3$, by applying the above corollary, we get the following corollary.

Corollary 24. *For any integer $1 \leq t, k \leq n$, any integer $r \leq \frac{\log n - \log t - \log k}{\log \log n + 3}$, there is no (n, r, t) -commit-and-reveal $(\frac{1}{nt}, n - k)$ -maximin-fair committee election protocol.*

6 Lower Bounds for Perfect Fairness

We recall that a n -party leader election protocol is perfectly fair against k -party corruption if and only if it is $(1, k)$ -fair, i.e., the probability of any honest party being selected is at least $1/n$ if the number of corrupted party is at most k . We first show that even if only one party is corrupted, there is no single-round perfectly fair leader election protocol. The prior impossibility results [3] by Chung et. al. only show it for the $(n - 1)$ -corruption case. Also, for multi-round protocols, we extend the prior results [3] to the case of k -corruption for $k < n - 1$ and show that there is no r -round perfectly fair leader election protocol against k -corruption for $r < \min\{\lceil \log n \rceil, \lceil \log k \rceil + 1\}$.

Notations. We define the following convenient notations to simplify our proofs. For any $\mathbf{x} \in (\{\perp\} \cup \Omega)^n$ and $y \in \{\perp\} \cup \Omega$, we use $(\mathbf{x} : x_i \leftarrow y)$ to denote a vector which is exactly the same as \mathbf{x} except the i -th entry of \mathbf{x} is changed to y . If multiple entries are changed, we denote it as $(\mathbf{x} : \{x_i \leftarrow y_i\}_{i \in S})$, where S is a subset of $[n]$.

6.1 Impossibility of Single-Round Protocols

Theorem 25. *For any $n \geq 3$ and $1 \leq k < n$, there is no perfectly fair single-round commit-and-reveal leader election protocol against k -corruption.*

Proof Sketch. Our proof can be divided in two steps. First, we show that for any $(1, k)$ -fair single-round commit-and-reveal leader election protocol Π , Π must be *abort-invariant*, i.e., the resulting leader will not change, if any party other than the leader aborts. Moreover, this implies that if any party i other than the resulting leader changes its input, the leader must be either the original leader or changed to i , which is formally stated in Lemma 26. Then, we show that this property implies that there must exist an input y^* for party i^* and another party $j^* \neq i^*$ such that if the input of party i^* is y^* , party j^* will never be the leader no matter how the other parties choose their inputs. This means that Π is not fair.

To find such (y^*, i^*, j^*) , we start from an arbitrary input \mathbf{x} of all parties. Suppose party i is selected given \mathbf{x} . We pick an arbitrary $j \neq i$ and attempt to find another input y of party j such that the leader is changed to party j if party j changes its input to y while the inputs of all other parties remain the same as \mathbf{x} . If such y does not exist, it means that j would never be selected no matter what input party j picks. Also, due to *abort-invariance* of Π , j would never be selected no matter how parties other than i and j choose their inputs given party i selects x_i . Therefore, $(y^* = x_i, i^* = i, j^* = j)$ is the tuple we want. If such y exists, we repeat the above for input $(\mathbf{x} : x_j \leftarrow y)$ until we find such a tuple.

We then show that the above process always terminates. Suppose it does not terminate. Since the input set is finite, we can find a loop of input-party pairs $(\mathbf{x}_1, i_1), \dots, (\mathbf{x}_\ell, i_\ell)$ with $(\mathbf{x}_1, i_1) = (\mathbf{x}_\ell, i_\ell)$ such that \mathbf{x}_k is the same as \mathbf{x}_{k-1} except that party i_k is selected given \mathbf{x}_k and the input of party i_k is changed. To yield a contradiction, the idea is to start from \mathbf{x}_1 and do all the changes in the loop except that we do not change the input of party i_1 . Equivalently, we consider an alternative loop $(\mathbf{x}'_1, i_1), \dots, (\mathbf{x}'_\ell, i_\ell)$ where $\mathbf{x}'_k := (\mathbf{x}_k : x_{k, i_1} \leftarrow x_{1, i_1})$. We show that for $i_k \neq i_1$, given \mathbf{x}'_k , party i_k is still selected. Then, since $i_{\ell-1} \neq i_\ell = i_1$, it implies that party $i_{\ell-1}$ is selected given $\mathbf{x}'_{\ell-1}$. However, since $\mathbf{x}_1 = \mathbf{x}'_\ell = \mathbf{x}'_{\ell-1}$, party i_1 should be selected given $\mathbf{x}'_{\ell-1}$, which yields a contradiction.

Lemma 26. *Suppose $\Pi : (\{\perp\} \cup \Omega)^n \rightarrow \{0, 1\}^n$ is a perfectly maximin-fair n -party single-round commit-and-reveal leader election protocol against a single-party corruption. Π must be abort-invariant, i.e., for any $\mathbf{x} \in \Omega^n$ and $i \in [n]$ such that $\Pi_i(\mathbf{x}) = 0$, it holds that $\Pi_j(\mathbf{x} : x_i \leftarrow \perp) = \Pi_j(\mathbf{x})$ for any $j \in [n]$. Moreover, abort-invariant implies, for any $\mathbf{x} \in \Omega^n$, $y \in \Omega$, if $\Pi_i(\mathbf{x}) = \Pi_i(\mathbf{x} : x_i \leftarrow y) = 0$, i.e., party i is not selected given \mathbf{x} or $(\mathbf{x} : x_i \leftarrow y)$, then $\Pi_j(\mathbf{x} : x_i \leftarrow y) = \Pi_j(\mathbf{x})$ for any $j \in [n]$.*

Proof (Lemma 26). Suppose Π is not abort-invariant, which means there exists $\mathbf{x} \in \Omega^n$ and $i, j \in [n]$ such that $\Pi_i(\mathbf{x}) = 0$, $\Pi_j(\mathbf{x}) = 1$, and $\Pi_j(\mathbf{x} : x_i \leftarrow \perp) = 0$. We construct an adversary \mathcal{A} as follows. \mathcal{A} corrupts party i and lets party i run the protocol honestly except party i aborts if the inputs of all parties are exactly \mathbf{x} . Then, the probability that party j is selected as the leader is smaller than the probability that party j is selected when all parties behave honestly, which is exactly $1/n$. Therefore, the protocol is not perfectly fair.

We now show the “moreover” part. For any $\mathbf{x} \in \Omega^n$, $y \in \Omega$, and $i \in [n]$ such that $\Pi_i(\mathbf{x} : x_i \leftarrow y) = 0$, since Π is abort-invariant, we have $\Pi_j(\mathbf{x} : x_i \leftarrow y) = \Pi_j(\mathbf{x} : x_i \leftarrow \perp) = \Pi_j(\mathbf{x})$ for any $j \in [n]$. \square

Proof (Theorem 25). Suppose $\Pi : (\{\perp\} \cup \Omega)^n \rightarrow \{0, 1\}^n$ is a n -party single-round commit-and-reveal leader election protocol. We just need to show that there exists an input $y^* \in \Omega$ for some party i^* and another party $j^* \neq i^*$ such that $\Pi_{j^*}(\mathbf{x}) = 0$ for all $\mathbf{x} \in \Omega^n$ with $x_{i^*} = y^*$, which implies that Π is not fair.

We use the following algorithm to find (i^*, y^*, j^*) ; The algorithm is not efficient, but it is sufficient in order to show the existence of (i^*, y^*, j^*) . Initially, the algorithm picks an arbitrary input $\mathbf{x}_0 \in \Omega^n$. We denote i_0 as the leader given \mathbf{x}_0 as the inputs of all parties and $y_0 := x_{0, i_0}$ as the input of party i_0 . Then, we keep iterating the following. At the ℓ -th iteration, since $n \geq 3$, the algorithm picks an arbitrary $i_\ell \in [n] \setminus \{i_{\ell-1}, i_{\ell-2}\}$. (For the first iteration, the algorithm picks an arbitrary $i_1 \in [n] \setminus \{i_0\}$.) Then, it finds y_ℓ such that party i_ℓ is the leader given $\mathbf{x}_\ell := (\mathbf{x}_{\ell-1} : x_{\ell-1, i_\ell} \leftarrow y_\ell)$ as the inputs of all parties, i.e., the input of party i_ℓ is changed to y_ℓ while the inputs of all other parties remain the same as $\mathbf{x}_{\ell-1}$. If such y_ℓ does not exist, then the algorithm returns $(i^* \leftarrow i_{\ell-1}, y^* \leftarrow y_{\ell-1}, j^* \leftarrow i_\ell)$.

We first show that (i^*, y^*, j^*) returned by the algorithm satisfies the property mentioned at the beginning of the proof. Denote $\mathbf{x}^* := \mathbf{x}_{\ell-1}$. By the execution of the algorithm, party j^* is not selected given input \mathbf{x}^* . For any $\mathbf{x} \in \Omega^n$ with $x_1 = y^*$, we change \mathbf{x}^* step by step to make it equal to \mathbf{x} and party j^* remains not the leader. First, we change the input of party j^* in \mathbf{x}^* to x_{j^*} . By the execution of the algorithm, party i^* remains the leader. Then, by Lemma 26, the leader is not changed to j^* if party $k \in [n] \setminus \{i^*, j^*\}$ changes its input to x_k , which concludes our claim.

It is left to show the algorithm always returns. Suppose the algorithm does not return. Since the input space is finite, the algorithm must find a loop $(i_\ell, \mathbf{x}_\ell, y_\ell), \dots, (i_m, \mathbf{x}_m, y_m)$ such that $(i_\ell, \mathbf{x}_\ell, y_\ell) = (i_m, \mathbf{x}_m, y_m)$. We now show that such a loop cannot exist. By the execution of the algorithm, it holds that \mathbf{x}_{j+1} is the same as \mathbf{x}_j except that the input of party i_{j+1} is changed to y_{j+1} for $\ell \leq j < m$ and party i_j is leader given the input \mathbf{x}_j for $\ell \leq j \leq m$.

To yield a contradiction, we consider the following loop of inputs $(\tilde{\mathbf{x}}_\ell, \dots, \tilde{\mathbf{x}}_m)$, where $\tilde{\mathbf{x}}_j$ is the same as \mathbf{x}_j except that the input of party i_ℓ is changed to y_ℓ , i.e., $\tilde{\mathbf{x}}_j := \mathbf{x}_j : x_{j, i_\ell} \leftarrow y_\ell$. We will show that party i_ℓ is not selected as the leader given input $\tilde{\mathbf{x}}_j$ for any $\ell < j \leq m$. It yields a contradiction since party i_ℓ is selected as the leader given input $\mathbf{x}_j = \tilde{\mathbf{x}}_\ell = \tilde{\mathbf{x}}_m$. More precisely, we are going to show that for any $\ell + 1 \leq j \leq m$, if $i_j \neq i_\ell$, then party i_j is selected given $\tilde{\mathbf{x}}_j$, and if $i_j = i_\ell$, then party $i_{j-1} (\neq i_j = i_\ell)$ is selected given $\tilde{\mathbf{x}}_j$.

First, for $j = \ell + 1$, since $i_{\ell+1} \neq i_\ell$, we know $\tilde{\mathbf{x}}_{\ell+1} = \mathbf{x}_{\ell+1}$. Therefore, party i_j is selected given $\tilde{\mathbf{x}}_j$.

For $j > \ell + 1$, there are three cases: (i) $i_{j-1} \neq i_\ell$ and $i_j \neq i_\ell$; (ii) $i_{j-1} \neq i_\ell$ and $i_j = i_\ell$; (iii) $i_{j-1} = i_\ell$. For the first two cases, suppose party i_{j-1} is selected given $\tilde{\mathbf{x}}_{j-1}$. If $i_j \neq i_\ell$, since both party i_ℓ and party i_j are not selected given $\tilde{\mathbf{x}}_{j-1}$, by Lemma 26, party i_ℓ is also not selected given $\tilde{\mathbf{x}}_j = (\tilde{\mathbf{x}}_{j-1} : \tilde{x}_{j-1, i_j} \leftarrow y_j)$.

Then, since $\tilde{\mathbf{x}}_j = (\mathbf{x}_j : x_{j,i_\ell} \leftarrow y_\ell)$, by Lemma 26, we have $\Pi_{i_j}(\tilde{\mathbf{x}}_j) = \Pi_{i_j}(\mathbf{x}_j) = 1$. Otherwise, if $i_j = i_\ell$, we have $\tilde{\mathbf{x}}_{j-1} = \tilde{\mathbf{x}}_j$ and thus party i_{j-1} is selected given $\tilde{\mathbf{x}}_j$.

For case (iii), suppose party i_{j-2} is selected given $\tilde{\mathbf{x}}_{j-1}$. By the execution of the algorithm, we know $i_j, i_{j-1}(= i_\ell), i_{j-2}$ are distinct. Since both party i_ℓ and party i_j are not the leader given the inputs $\tilde{\mathbf{x}}_{j-1}$, by Lemma 26, party i_ℓ is not selected either given $\tilde{\mathbf{x}}_j = (\tilde{\mathbf{x}}_{j-1} : \tilde{x}_{j-1,i_j} \leftarrow y_j)$. Then, since $\tilde{\mathbf{x}}_j = (\mathbf{x}_j : x_{j,i_\ell} \leftarrow y_\ell)$, by Lemma 26, we have $\Pi_{i_j}(\tilde{\mathbf{x}}_j) = \Pi_{i_j}(\mathbf{x}_j) = 1$. Therefore, we can conclude the statement by induction. \square

6.2 Lower Bounds for Multi-Round Protocols

For multi-round protocols, the prior result [3] by Chung et. al. shows that there is no perfectly fair $(\lceil \log n \rceil - 1)$ -round leader election protocol against $(n - 1)$ -corruption. We show that their result can be extended to any k -corruption for $k \geq n/2$. Also, for $2 \leq k < n/2$, we show there is no perfectly fair $\lceil \log k \rceil$ -round protocol. Formally, we show Theorem 27. We also note that this result is incomparable to our result for the single-round case since the statement is trivial for $k = 1$.

Theorem 27. *For any $2 \leq k \leq n$, there is no perfectly fair r -round commit-and-reveal leader election protocol against k -corruption for $r \leq \lceil \log(\min\{n/2, k\}) \rceil$.*

We prove a stronger statement: we show that the impossibility result holds even for protocols satisfying a weaker security notion, called *tightness*, which is introduced in [3]. We say a protocol is tight against k -corruption if and only if the winning probability of any honest party given k corrupted parties is as high as in honest executions, which is formally defined as follows. It is clear that a perfectly fair protocol against k -corruption is tight against k -corruption.⁶

Definition 28 ([3]). *A n -party leader election protocol Π is tight against k -corruption if and only if for any adversary \mathcal{A} that corrupts at most k parties and any honest party i , no matter how \mathcal{A} behaves,*

$$\Pr[i \text{ is the leader}] \geq \mathcal{P}_i,$$

where \mathcal{P}_i denotes the probability that party i is elected in an honest execution.

The proof technique is similar to [3]. We say that a party is still alive after i rounds if the party still has a chance to be the leader after i rounds. To show a lower bound on round complexity, the idea is to lower bound the number of alive parties. The prior work [3] shows that in a tight protocol against $(n - 1)$ -corruption, the number of alive parties after the first round is at least $n'/2$, where n' denotes the alive parties before the first round. Then, by fixing the first round

⁶ For a perfectly fair protocol, the winning probability of any party in an honest execution is $1/n$. Therefore, the winning probability of any honest party i given k corrupted parties is at least $\mathcal{P}_i = 1/n$.

input, one can show the rest of protocol is still tight, and the same argument shows that the number of alive parties after i round is at least $n'/2^i$. Since in the final round, the number of alive parties is 1 and thus the round complexity of a tight protocol is at least $\lceil \log(n') \rceil$.

We extend the prior proof to the case of k -corruption and show that the number of alive parties after the first round is at least $\min\{n'/2, k\}$.⁷ By a similar induction, we conclude that the round complexity is at least $\lceil \log(\min\{n'/2, k\}) \rceil$ and for perfectly fair protocols, we have $n' = n$.

Remark 29. We also note that the technique here is different from the previous section on the single-round protocols. The single-round result shows that the number of alive parties after the first round is at least 2 given that one party is corrupted. However, it is unclear how to improve this bound for larger corruptions.

Proof (Theorem 27). Let $\Pi : (\{\perp\} \cup \Omega)^{nr} \rightarrow \{0, 1\}^n$ be a r -round commit-and-reveal leader election protocol. For any $\mathbf{x} \in (\{\perp\} \cup \Omega)^n$, denote $\mathcal{P}_i(\mathbf{x})$ as the probability that party i is elected in an honest execution given that the first-round inputs of all parties are \mathbf{x} . We say that party i is eliminated if $\mathcal{P}_i(\mathbf{x}) = 0$. Otherwise, we say that the party i is still alive. Denote $\mathcal{S}(\mathbf{x}) := \{i \in [n] \mid \mathcal{P}_i(\mathbf{x}) > 0\}$ as the set of the alive parties. Also, we denote $\mathcal{S}_0 := \bigcup_{\mathbf{x} \in \Omega^n} \mathcal{S}(\mathbf{x})$, which is the set of parties that are alive before the first round, and denote $n' = |\mathcal{S}_0|$. We say Π is a protocol with n' alive parties.

We first show the the following lemma which generalizes the abort-invariant property of single-round leader election protocols (Lemma 26) to the multi-round case. Roughly, the abort-invariance means that for any first-round input \mathbf{x} , an eliminated party i given \mathbf{x} , and $j \neq i$, $\mathcal{P}_j(\mathbf{x})$ would not change if party i aborts, and moreover, it implies that if party i changes its input, $\mathcal{P}_j(\mathbf{x})$ would only decrease. The proof is similar to the single-round case and deferred to the end of the section.

Lemma 30. *Suppose $\Pi : (\{\perp\} \cup \Omega)^n \rightarrow \{0, 1\}^n$ is a tight n -party commit-and-reveal leader election protocol against a single-party corruption. Π must be abort-invariant, i.e., for any $\mathbf{x} \in \Omega^n$ and $i \in [n]$ such that $\mathcal{P}_i(\mathbf{x}) = 0$, it holds that $\mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp) = \mathcal{P}_j(\mathbf{x})$ for any $j \in [n]$. Moreover, for any $y \in \Omega$, $\mathcal{P}_j(\mathbf{x} : x_i \leftarrow y) \leq \mathcal{P}_j(\mathbf{x})$ for any $j \in [n] \setminus \{i\}$.*

We use the lemma to show the following claim.

Claim. If Π is tight, then there exists $\mathbf{x} \in \Omega^n$ such that $|\mathcal{S}(\mathbf{x})| \geq \min\{n'/2, k\}$.

Proof. Let $\mathbf{x}_0 \in \Omega^n$ be an arbitrary input. Without loss of generality, assume $\mathcal{S}_0 = \{1, \dots, n'\}$ and $\mathcal{S}(\mathbf{x}_0) = \{1, \dots, \ell\}$. The claim holds if $\ell \geq \min\{n'/2, k\}$. Otherwise, we run the following algorithm to find \mathbf{x} such that $|\mathcal{S}(\mathbf{x})| \geq \min\{n'/2, k\}$. For $1 \leq i \leq n' - \ell$, the algorithm finds $y_i \in \Omega$ such that party $\ell + i$ becomes alive

⁷ Note that this statement is only useful when $k \geq 2$. For $k = 1$, it means the number of alive parties after the first round is at least 1, which holds trivially.

after it changes its first round input to y_i , i.e., $\mathcal{P}_{\ell+i}(\mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow y_i) > 0$ and sets $\mathbf{x}_i := \mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow y_i$. The algorithm returns \mathbf{x}_i if $|\mathcal{S}(\mathbf{x}_i)| \geq \min\{n/2, k\}$.

We first show that the algorithm can find y_i for each i . Suppose for any $y \in \Omega$ such that $\mathcal{P}_{\ell+i}(\mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow y) = 0$. Since the algorithm did not return, we know $|\mathcal{S}(\mathbf{x}_{i-1})| < \min\{n'/2, k\}$. For any $\mathbf{x}' \in \Omega^n$ such that $x'_j = x_{i-1,j}$ for each $j \in \mathcal{S}(\mathbf{x}_{i-1})$, we show that $\mathcal{P}_{\ell+i}(\mathbf{x}') = 0$. First, if we change the input of party $\ell + i$ to $x'_{\ell+i}$, we have $\mathcal{P}_{\ell+i}(\mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow x'_{\ell+i}) = 0$. Denote $\mathbf{x}'' = \mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow x'_{\ell+i}$. By Lemma 30, if we change the input of each party $j \in [n] \setminus (\{\ell + i\} \cup \mathcal{S}(\mathbf{x}_{i-1}))$ from x''_j to x'_j , the probability that party $i + \ell$ is the leader is still 0, which implies $\mathcal{P}_{\ell+i}(\mathbf{x}') = 0$. This shows that Π is not tight, since the adversary can prevent party $\ell + i$ from being selected by corrupting all parties in $\mathcal{S}(\mathbf{x}_{i-1})$ and setting their first-round inputs to be the same as \mathbf{x}_{i-1} .

We now show that the algorithm always returns. For $1 \leq i \leq n' - \ell$, we show that $j \in \mathcal{S}(\mathbf{x}_i)$ for each $\ell + 1 \leq j \leq \ell + i$, which implies that the algorithm must return when $i = \min\{n'/2, k\} \leq n' - \ell$. For each $1 \leq i \leq n' - \ell$, suppose $j \in \mathcal{S}(\mathbf{x}_{i-1})$ for each $\ell + 1 \leq j \leq \ell + i - 1$, which trivially holds for $i = 1$. Denote $\mathcal{D} := \{\mathbf{x} \in \Omega^n \mid x_j = x_{0,j} \text{ for } j \in [\ell] \cup \{\ell + i\}\}$. For each $\mathbf{x}' \in \mathcal{D}$, since all parties in $[(\ell + 1)..n] \setminus \{\ell + i\}$ are eliminated given \mathbf{x}_0 , by Lemma 30, we know $\mathcal{P}_{\ell+i}(\mathbf{x}') = \mathcal{P}_{\ell+i}(\mathbf{x}_0 : \{x_{0,j} \leftarrow x'_j\}_{j \in [(\ell+1)..n] \setminus \{\ell+i\}}) \leq \mathcal{P}_{\ell+i}(\mathbf{x}_0) = 0$, which means party $\ell + i$ is eliminated given any input $\mathbf{x}' \in \mathcal{D}$. Then, by Lemma 30, for any $j \in [n] \setminus \{\ell + i\}$

$$\mathcal{P}_j(\mathbf{x}' : x'_{\ell+i} \leftarrow y_i) \leq \mathcal{P}_j(\mathbf{x}') . \quad (4)$$

Since Π is tight, it holds that for any $j \in [(\ell + 1)..n] \setminus \{\ell + i\}$ and any $y \in \Omega$,

$$\mathbb{E}_{\mathbf{x}' \sim \mathcal{D}}[\mathcal{P}_j(\mathbf{x}')] = \mathbb{E}_{\mathbf{x}' \sim \mathcal{D}}[\mathcal{P}_j(\mathbf{x}' : x'_{\ell+i} \leftarrow y)] ,$$

since otherwise the adversary can decrease the chance that party j is selected by corrupting parties $[\ell] \cup \{\ell + i\}$ (the number of which is at most k) and letting the input of parties $[\ell]$ be that same as \mathbf{x}' and the input of party $\ell + i$ be y that gives the worst expectation. Therefore, by Equation (4), we have $\mathcal{P}_j(\mathbf{x}' : x'_{\ell+i} \leftarrow y_i) = \mathcal{P}_j(\mathbf{x}')$ for each $\mathbf{x}' \in \mathcal{D}$. Since $\mathbf{x}_{i-1} \in \mathcal{D}$ and $\mathcal{P}_j(\mathbf{x}_{i-1}) > 0$ for each $\ell + 1 \leq j \leq \ell + i - 1$, we have $\mathcal{P}_j(\mathbf{x}_i) = \mathcal{P}_j(\mathbf{x}_{i-1} : x_{i-1,\ell+i} \leftarrow y_i) = \mathcal{P}_j(\mathbf{x}_{i-1}) > 0$. Also, since $\mathcal{P}_{\ell+i}(\mathbf{x}_i) > 0$, we have $j \in \mathcal{S}(\mathbf{x}_i)$ for each $\ell + 1 \leq j \leq \ell + i$. Therefore, we can conclude the statement by induction. \square

We now show that for any tight protocol Π with n' alive parties, the round complexity of Π is at least $\lceil \log(\min\{n'/2, k\}) \rceil$ by doing induction on n' . For $n' = 1$, which means the leader is already determined at the beginning, the statement holds trivially since $r \geq 0$. For $n' > 1$, suppose the statement holds for smaller n' and Π is a protocol with n' alive parties and optimal round complexity. By the claim, there exists $\mathbf{x} \in \Omega^n$ such that $|\mathcal{S}(\mathbf{x})| \geq \min\{n'/2, k\}$. Given that the first-round inputs is \mathbf{x} , we can view the rest of the execution of Π as a $(r - 1)$ -round leader election protocol. Denote the resulting protocol as Π' . It is not hard to show that Π' is also tight and the number of alive parties of Π' before

the first round is $|\mathcal{S}(\mathbf{x})|$. Since Π is round optimal, we have $|\mathcal{S}(\mathbf{x})| < n'$. By our assumption, the round complexity of Π' is at least $\lceil \log(\min\{|\mathcal{S}(\mathbf{x})|/2, k\}) \rceil \geq \lceil \log(\min\{n'/4, k/2, k\}) \rceil = \lceil \log(\min\{n'/2, k\}/2) \rceil = \lceil \log(\min\{n'/2, k\}) \rceil - 1$, which implies the round complexity of Π is at least $\lceil \log(\min\{n'/2, k\}) \rceil$. We can conclude the theorem since a perfectly fair n -party protocol against k -corruption is a tight protocol against k -corruption with n alive parties. \square

Proof (Lemma 30). Suppose Π is not abort-invariant, which means there exists $\mathbf{x} \in \Omega^n$ and $i \neq j \in [n]$ such that $\mathcal{P}_i(\mathbf{x}) = 0$, $\mathcal{P}_j(\mathbf{x}) \neq \mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp)$. Without loss of generality we can assume $\mathcal{P}_j(\mathbf{x}) > \mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp)$.⁸ We construct an adversary \mathcal{A} as follows. \mathcal{A} corrupts party i and lets party i run the protocol honestly except party i aborts if the inputs of all parties are exactly \mathbf{x} . Then, the probability that party j is selected as the leader

$$\begin{aligned} & \Pr_{\mathbf{x}' \sim \Omega^n} [\mathbf{x} = \mathbf{x}'] \cdot \mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp) + \sum_{\mathbf{z} \neq \mathbf{x} \in \Omega^n} \Pr_{\mathbf{x}' \sim \Omega^n} [\mathbf{z} = \mathbf{x}'] \cdot \mathcal{P}_j(\mathbf{z}) \\ & < \Pr_{\mathbf{x}' \sim \Omega^n} [\mathbf{x} = \mathbf{x}'] \cdot \mathcal{P}_j(\mathbf{x}) + \sum_{\mathbf{z} \neq \mathbf{x} \in \Omega^n} \Pr_{\mathbf{x}' \sim \Omega^n} [\mathbf{z} = \mathbf{x}'] \cdot \mathcal{P}_j(\mathbf{z}) \\ & = \sum_{\mathbf{z} \in \Omega^n} \Pr_{\mathbf{x}' \sim \Omega^n} [\mathbf{z} = \mathbf{x}'] \cdot \mathcal{P}_j(\mathbf{z}) = \mathcal{P}_j, \end{aligned}$$

where \mathcal{P}_j is the probability that party j is selected in an honest execution. Therefore, the protocol is not tight.

For the “moreover” part, suppose there exists $y \in \Omega$ and $j \in [n] \setminus \{i\}$ such that $\mathcal{P}_j(\mathbf{x} : x_i \leftarrow y) > \mathcal{P}_j(\mathbf{x})$. Since Π is abort-invariant, we have $\mathcal{P}_j(\mathbf{x} : x_i \leftarrow y) > \mathcal{P}_j(\mathbf{x}) = \mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp)$. Let $\hat{\mathbf{x}} := (\mathbf{x} : x_i \leftarrow y)$. Then, $\mathcal{P}_j(\hat{\mathbf{x}}) < \mathcal{P}_j(\hat{\mathbf{x}} : \hat{x}_i \leftarrow \perp)$. Therefore, we can use the same argument from the first part to construct an adversary \mathcal{A} that breaks the tightness of Π . \square

Acknowledgments

Klein and Komargodski were supported in part by an Alon Young Faculty Fellowship, by a grant from the Israel Science Foundation (ISF Grant No. 1774/20), by a grant from the US-Israel Binational Science Foundation and the US National Science Foundation (BSF-NSF Grant No. 2020643), and by the European Union (ERC, SCALE,101162665). Ilan Komargodski is the Incumbent of the Harry & Abe Sherman Senior Lectureship at the School of Computer Science and Engineering at the Hebrew University. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them. Zhu was supported in part by NSF grants CNS-2026774, CNS-2154174, a JP Morgan Faculty Award, a CISCO Faculty Award, and a gift from Microsoft.

⁸ Otherwise, since $\sum_{k \in [n] \setminus i} \mathcal{P}_k(\mathbf{x}) = 1 = \sum_{k \in [n] \setminus i} \mathcal{P}_k(\mathbf{x} : x_i \leftarrow \perp)$, if there exists j such that $\mathcal{P}_j(\mathbf{x}) < \mathcal{P}_j(\mathbf{x} : x_i \leftarrow \perp)$, there also exists j' such that $\mathcal{P}_{j'}(\mathbf{x}) > \mathcal{P}_{j'}(\mathbf{x} : x_i \leftarrow \perp)$.

References

1. Berman, I., Haitner, I., Tentes, A.: Coin flipping of any constant bias implies one-way functions. *J. ACM* **65**(3) (Mar 2018). <https://doi.org/10.1145/2979676>, <https://doi.org/10.1145/2979676>
2. Blum, M.: Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News* **15**(1), 23–27 (Jan 1983). <https://doi.org/10.1145/1008908.1008911>, <https://doi.org/10.1145/1008908.1008911>
3. Chung, K.M., Chan, T.H.H., Wen, T., Shi, E.: Game-theoretic fairness meets multi-party protocols: The case of leader election. In: Malkin, T., Peikert, C. (eds.) *CRYPTO 2021, Part II*. LNCS, vol. 12826, pp. 3–32. Springer, Cham, Virtual Event (Aug 2021). https://doi.org/10.1007/978-3-030-84245-1_1
4. Chung, K.M., Guo, Y., Lin, W.K., Pass, R., Shi, E.: Game theoretic notions of fairness in multi-party coin toss. In: Beimel, A., Dziembowski, S. (eds.) *TCC 2018, Part I*. LNCS, vol. 11239, pp. 563–596. Springer, Cham (Nov 2018). https://doi.org/10.1007/978-3-030-03807-6_21
5. Cleve, R.: Limits on the security of coin flips when half the processors are faulty (extended abstract). In: *18th ACM STOC*. pp. 364–369. ACM Press (May 1986). <https://doi.org/10.1145/12130.12168>
6. Feige, U.: Noncryptographic selection protocols. In: *40th FOCS*. pp. 142–153. IEEE Computer Society Press (Oct 1999). <https://doi.org/10.1109/SFFCS.1999.814586>
7. Filmus, Y., Hambardzumyan, L., Hatami, H., Hatami, P., Zuckerman, D.: Biasing boolean functions and collective coin-flipping protocols over arbitrary product distributions. *CoRR* **abs/1902.07426** (2019), <http://arxiv.org/abs/1902.07426>
8. Gelashvili, R., Goren, G., Spiegelman, A.: Short paper: On game-theoretically-fair leader election. In: Eyal, I., Garay, J.A. (eds.) *FC 2022*. LNCS, vol. 13411, pp. 531–538. Springer, Cham (May 2022). https://doi.org/10.1007/978-3-031-18283-9_26
9. Goldreich, O., Goldwasser, S., Linial, N.: Fault-tolerant computation in the full information model. *SIAM Journal on Computing* **27**(2), 506–544 (1998)
10. Gradwohl, R., Vadhan, S., Zuckerman, D.: Random selection with an adversarial majority. In: Dwork, C. (ed.) *CRYPTO 2006*. LNCS, vol. 4117, pp. 409–426. Springer, Berlin, Heidelberg (Aug 2006). https://doi.org/10.1007/11818175_25
11. Haitner, I., Omri, E.: Coin flipping with constant bias implies one-way functions. In: Ostrovsky, R. (ed.) *52nd FOCS*. pp. 110–119. IEEE Computer Society Press (Oct 2011). <https://doi.org/10.1109/FOCS.2011.29>
12. Komargodski, I., Matsuo, S., Shi, E., Wu, K.: \log^* -round game-theoretically-fair leader election. In: Dodis, Y., Shrimpton, T. (eds.) *CRYPTO 2022, Part III*. LNCS, vol. 13509, pp. 409–438. Springer, Cham (Aug 2022). https://doi.org/10.1007/978-3-031-15982-4_14
13. v. Neumann, J.: Zur theorie der gesellschaftsspiele. *Mathematische annalen* **100**(1), 295–320 (1928)
14. Russell, A., Saks, M.E., Zuckerman, D.: Lower bounds for leader election and collective coin-flipping in the perfect information model. In: *31st ACM STOC*. pp. 339–347. ACM Press (May 1999). <https://doi.org/10.1145/301250.301337>
15. Russell, A., Zuckerman, D.: Perfect information leader election in $\log^*n + O(1)$ rounds. In: *39th FOCS*. pp. 576–583. IEEE Computer Society Press (Nov 1998). <https://doi.org/10.1109/SFCS.1998.743508>

16. Sanghvi, S., Vadhan, S.P.: The round complexity of two-party random selection. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 338–347. ACM Press (May 2005). <https://doi.org/10.1145/1060590.1060641>
17. Wu, K., Asharov, G., Shi, E.: A complete characterization of game-theoretically fair, multi-party coin toss. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part I. LNCS, vol. 13275, pp. 120–149. Springer, Cham (May / Jun 2022). https://doi.org/10.1007/978-3-031-06944-4_5