Electronic Colloquium on Computational Complexity, Revision 4 of Report No. 168 (2017)

Tighter Bounds on Multi-Party Coin Flipping via Augmented Weak Martingales and Differentially Private Sampling

Amos Beimel* Iftach Haitner†‡ Nikolaos Makriyannis§‡ Eran Omri¶

November 5, 2017

Abstract

In his seminal work, Cleve [STOC '86] has proved that any r-round coin-flipping protocol can be efficiently biassed by $\Theta(1/r)$. The above lower bound was met for the two-party case by Moran, Naor, and Segev [Journal of Cryptology '16], and the three-party case (up to a polylog factor) by Haitner and Tsfadia [SICOMP '17], and was approached for n-party protocols when $n < \log\log r$ by Buchbinder, Haitner, Levi, and Tsfadia [SODA '17]. For $n > \log\log r$, however, the best bias for n-party coin-flipping protocols remains $O(n/\sqrt{r})$ achieved by the majority protocol of Awerbuch, Blum, Chor, Goldwasser, and Micali [Manuscript '85].

Our main result is a tighter lower bound on the bias of coin-flipping protocols, showing that, for every constant $\varepsilon > 0$, an r^{ε}-party r-round coin-flipping protocol can be efficiently biased by $\widetilde{\Omega}(1/\sqrt{r})$. As far as we know, this is the first improvement of Cleve's bound that holds in the standard model, and is only $n = r^{\varepsilon}$ (multiplicative) far from the aforementioned upper bound of Awerbuch et al.

For proving the above lower bound we present two new results that we believe are of independent interest. The first result is that a sequence of (augmented) weak martingales have large gap: with constant probability there exists two adjacent variables whose gap is at least the ratio between the gap between the first and last variables and the square root of the number of variables. This generalizes the result of Cleve and Impagliazzo [Manuscript '93], who proved that the above holds for strong martingales. The second result is a new sampling algorithm that uses a differentially private mechanism to minimize the effect of data divergence.

Keywords: multi-party computation; coin-flipping; augmented weak martingales; differential privacy; oblivious sampling;

*Department of Computer Science, Ben Gurion University. E-mail: amos.beimel@gmail.com. Research supported by ISF grants 544/13 and 152/17.

†School of Computer Science, Tel Aviv University. E-mail: iftachh@cs.tau.ac.il. Member of the Israeli Center of Research Excellence in Algorithms (ICORE) and the Check Point Institute for Information Security.

‡Research supported by ERC starting grant 638121.

§School of Computer Science, Tel Aviv University. E-mail: n.makriyannis@gmail.com

¶Department of Computer Science, Ariel University. E-mail: omrier@ariel.ac.il. Research supported by ISF grants 544/13 and 152/17.

ISSN 1433-8092

Contents

1 Introduction

In a multi-party coin-flipping protocol, introduced by Blum [8], the parties wish to output a common (close to) unbiased bit, even though some of the parties may be corrupted and try to bias the output. More formally, such protocols should satisfy the following two properties: first, when all parties are honest (i.e., follow the prescribed protocol), they all output the *same* unbiased bit. Second, even when some parties are corrupted (i.e., collude and arbitrarily deviate from the protocol), the remaining parties should still output the same bit, and this bit should not be too biased (i.e., its distribution should be close to being uniform over $\{0,1\}$). We emphasize that the above requirements stipulate that the honest parties should *always* output a common bit, regardless of what the corrupted parties do, and in particular they are not allowed to abort if a cheat was detected.[1] Understanding coin flipping is important since it is a fundamental primitive with numerous cryptographic applications, and since lower bounds on such protocols imply the same bounds on many other basic cryptographic primitives including input-less primitives and the secure computation of many functions (e.g., the XOR function).

In his seminal work, Cleve [10] showed that for *any* efficient two-party r-round coin-flipping protocol, there exists an efficient fail-stop adversarial strategy (the adversary follows the protocol, but might abort prematurely) that biases the output of the honest party by $\Theta(1/r)$. Cleve further extended this lower bound to the multi-party case, with no honest majority, via a simple reduction. The above lower bound on coin-flipping protocols was met for the two-party case by Moran, Naor, and Segev [24] and for the three-party case (up to a polylog factor) by Haitner and Tsfadia [21], and was approached for n-party coin-flipping protocols when $n < \operatorname{loglog} r$ by Buchbinder, Haitner, Levi, and Tsfadia [9]. For $n > \operatorname{loglog} r$, however, the smallest bias for n-party coin-flipping protocol remains $O(n/\sqrt{r})$ achieved by the majority protocol of Awerbuch, Blum, Chor, Goldwasser, and Micali [5].

1.1 Our Results

Our main result is the following lower bound on the security of coin-flipping protocols.

Theorem 1.1 (Main result, informal)**.** *For any n-party r-round coin-flipping protocol with $n^k \geq r$, for some $k > 0$, there exists a fail-stop adversary running in time n^k that by corrupting a subset of the parties biases the outcome of honest parties by $1/(\sqrt{r} \cdot \log(r)^k)$.*

As a concrete example, assume the number of parties is $n = r^{1/100}$. The above theorem yields an attack of bias $\widetilde{\Omega}(1/\sqrt{r}) = \widetilde{\Omega}(1/r^{.5})$, to be compare to the $n/\sqrt{r} = 1/r^{.49}$ upper bound of Awerbuch et al. [5]. As far as we know, Theorem 1.1 is the first improvement over the $\Omega(1/r)$ bound of Cleve [10] that holds in the standard model (i.e., where parties are PPTM).

To prove Theorem 1.1, we prove the following two results that we believe to be found of independent interest.

1.1.1 Augmented Weak Martingale Has Large Gap

A sequence $X_1, \ldots, X_r$ of random variable is a *martingale*, if $\mathbf{E}[X_i \mid X_{\leq i-1}] = X_{i-1}$ for every $i \in [r]$ (letting $X_{\leq j} = (X_1, \ldots, X_j)$). Since we later consider relaxations of this notion, we henceforth

[1] Such protocols are typically addressed as having *guaranteed output delivery*, or, abusing notation, as *fair*. In the literature there are also weaker variants of coin-flipping protocols.

call such martingales *strong*. Cleve and Impagliazzo [11] have shown that any strong martingale sequence with $X_1 = \frac{1}{2}$ and $X_r \in \{0,1\}$, has a $1/\sqrt{r}$ gap with constant probability: with constant probability $|X_i - X_{i-1}| \geq \Omega(1/\sqrt{r})$ for some $i \in [r]$. This result is the core of their proof that there is an *inefficient* fail-stop attack on any coin-flipping protocol (see Section 1.2). The above theorem is typically used with respect to the *Doob martingale* sequence defined by $X_i = \mathbf{E}[f(Z_{\leq r}) \mid Z_{\leq i}]$, for arbitrary random variables $Z_1, \ldots, Z_r$ and function f of interest. To be applicable by efficient algorithms, however, requires that the value $X_i = \mathbf{E}[f(Z_{\leq r}) \mid Z_{\leq i}]$ is an efficiently computable function of $Z_{\leq i}$. In many cases, including the one considered by [11], $\mathrm{Supp}(Z_{\leq i})$ is typically huge, and hence, this function is not efficiently computable.

A relaxation of martingales is the so-called *weak martingales*, defined by Nelson [25], where it is only required that $\mathbf{E}[X_i \mid X_{i-1}] = X_{i-1}$. Namely, the conditioning is only on the value of the preceding variable, and not on the whole "history". As in the case of (strong) martingales, for arbitrary $Z_1, \ldots, Z_r$ we can consider the *Doob weak martingale* sequence $X_i = \mathbf{E}[f(Z_{\leq r}) \mid Z_i, X_{i-1}]$. The advantage is that the domain size of the function for computing X_i is only of size $\mathrm{Supp}(Z_i) \times \mathrm{Supp}(X_{i-1})$. In many applications, we can use discretization to reduce the support size of X_i (i.e., we let X_i be a *rounding* of $\mathbf{E}[f(Z_{\leq r}) \mid Z_i, X_{i-1}]$). Hence, if the support of Z_i is small, the computation of the X_i's can be done efficiently. (Such a discretization is not useful for the (strong) Doob martingales described above, since even if the support of each individual Z_1 is small (even 1), the domain of $Z_1, \ldots, Z_r$ is typically huge). Unfortunately, it is unclear whether weak martingale have large gaps, and thus we cannot facilitate the attack of Cleve and Impagliazzo [11] using such a sequence.

We prove that by somewhat strengthening the notion of Doob weak martingale we get a sequence that is still efficiently computable and at the same time has a large gap. A sequence $X_1, \ldots, X_r$ of random variable is a *χ-augmented weak martingales*, if $\mathbf{E}[X_i \mid X_{i-1}, \chi(X_{\leq i-1}))] = X_{i-1}$. The *Doob χ-augmented weak martingale* of $Z_1, \ldots, Z_r$ is defined by $X_i = \mathbf{E}_{Z_{1,\ldots,r}}[f(Z_{\leq r}) \mid Z_i, X_{i-1}, \chi(Z_{\leq i-1})]$.

If each of the Z_i's, f and χ have "small" (e.g., logarithmic) range and χ is efficiently computable, then X_i is efficiently computable. We prove that there exists a choice of χ for which Doob augmented weak martingales has a jump with constant probability.

Theorem 1.2 (Informal)**.** *For any sequence of random variables $Z_1, \ldots, Z_r$ and a function f, there exists a short-output function χ such that the following holds for the Doob χ-augmented weak martingale $X_1, \ldots, X_r$. If $f(\perp) = 1/2$ and $f(Z_1, \ldots, Z_r) \in \{0,1\}$, then $X_1, \ldots, X_r$ has a $1/\sqrt{r}$ gap with constant probability. Furthermore, the computation of X_i can be done in time $O(\max_i \{\mathrm{Supp}(X_i, Z_i)\})$.*

We prove that the above holds for a *rounded* variant of X_i, i.e., X_i is rounded to the closest multiplicative of some δ, which is not too small. Hence, if the support of the Z_i's small, the computation of the X_i's and of χ can be done efficiently. This efficiency plays a critical role in our attack on coin-flipping protocols, allowing us, in some cases, to employ an efficient variant of the attack of Cleve and Impagliazzo.

1.1.2 Exploiting Data Similarity in Oblivious Sampling via Differential Privacy

Consider the following r-round game in which your goal is to maximize the revenue of a random "party". In the beginning, a party H is chosen with uniform distribution from $\mathcal{H}$ (where $\mathcal{H}$ is a finite set of parties). In each round, values $\left\{s_i^h \in [0,1]\right\}_{h \in \mathcal{H}}$ are assigned to the parties of $\mathcal{H}$, but only the values $\{s_h\}_{h \in \mathcal{H} \setminus \{H\}}$ of the other parties are published. You can either decide to *abort* at

round i, and then party H is rewarded with s_i^H, or to continue to the next round. If you never choose to abort, then party H is rewarded with s_r^H (the value of the last round). You have the *similarity* guarantee that $\left|s_i^h - s_i\right| \leq \sigma$ for every $h \in \mathcal{H}$, where $s_i = \mathbf{E}_{h \leftarrow \mathcal{H}}\left[s_i^h\right]$. You are also guarantee that $\max_i \{s_i\} \geq \gamma$. A direct solution would be to decide to abort if the average of all other parties, i.e., $\{s_h\}_{h \in \mathcal{H} \setminus \{H\}}$, is larger than (roughly) $\gamma - \sigma$. The reward of this strategy is roughly $\gamma - \sigma$, and this linear loss in σ is inherent for this strategy.

We show that using a differentially private mechanism, and in particular adding Laplace noise to the estimated revenue, significantly improves upon the above. The idea is that by adding such noise, the identity of party H is kept somewhat secret, even given the aborting round. More accurately, the value of H is σ-*differentially private*, according to the definition of Dwork, McSherry, Nissim, and Smith [15]. We exploit this privacy guarantee to prove the following improvement in the expected reward.

Theorem 1.3 (Informal)**.** *Let $\left\{s_i^h \in [0,1]\right\}_{h \in \mathcal{H}, r \in [r]}$, σ, and $\gamma \geq 0$ be as above. Then there exists an efficient randomized strategy such that the expected reward for a random party in $\mathcal{H}$ is $\gamma - \sigma^2$.*

Namely, the penalty for having imperfect similarity is reduced from σ to σ^2. We also prove a generalization of the above where each party has a different similarity guarantee.

1.2 Our Technique

We describe the approach for proving Theorem 1.1 (our main result) using Theorems 1.2 and 1.3. For the proofs of the latter theorems see Sections 4 and 5 respectively.

Let Π be an r-round n-party coin-flipping protocol and let out denote the (always common) output of the parties in a random honest execution. By definition, $\mathsf{out} \in \{0,1\}$ and $\mathbf{E}[\mathsf{out}] = 1/2$. Our goal is to obtain an efficient attacker that, by controlling $n-1$ of the parties, biases the honest parties' output by $1/\sqrt{r}$ (we ignore log factors). We start by describing the $1/\sqrt{r}$ inefficient attack of Cleve and Impagliazzo [11].

1.2.1 Cleve and Impagliazzo's Attack

Let $n = 2$ and let $(\mathsf{P}_0, \mathsf{P}_1)$ be the parties of Π. Let $T_1, \ldots, T_r$ denote the messages in a random execution of Π. Let $X_i = \mathbf{E}[\mathsf{out} \mid T_{\leq i}]$; namely, X_i is the expected outcome of the protocol given $T_{\leq i} = T_1, \ldots, T_i$. It is easy to see that $X_1, \ldots, X_r$ is a (strong) martingale sequence. Hence, the result of [11], described in Section 1.1.1, yields that (omitting absolute values and constant factors)

$$\Pr\left[\, \exists i \in [r] \colon X_i - X_{i-1} \geq 1/\sqrt{r} \,\right] \in \Omega(1) \tag{1}$$

The martingale attack: Let the *backup* value Z_i^j denote the output of party P_j if the other party aborts *after* the i^{th} message was sent, letting $Z_r^j = Z_r^{\bar{j}}$ be the final output of P_j (when no abort occurs). Equation (1) yields that without loss of generality

$$\Pr\left[\exists i \in [r] \colon \mathsf{P}_j \text{ sends the } i^{\text{th}} \text{ message} \wedge \mathbf{E}\left[Z_{i-1}^{\bar{j}} \mid T_{\leq i}\right] - X_i \geq 1/2\sqrt{r}\right] \in \Omega(1) \tag{2}$$

Consider the attack that before sending the message T_i, party P_j aborts if $\mathbf{E}\left[Z^{\bar{j}}_{i-1} \mid T_{\leq i}\right] - X_i \geq 1/2\sqrt{r}$. By Equation (2) the above attack biases $\mathsf{P}_{\bar{j}}$ output towards one by $\Omega(1/2\sqrt{r})$.[2]

The clear limitation of the above attack is that in many cases, the value of both $X_i = \mathbf{E}\left[\mathsf{out} \mid T_{\leq i}\right]$ and $\mathbf{E}\left[Z^{\bar{j}}_i \mid T_{\leq i}\right]$ are *not* efficiently computable (given $T_{\leq i}$). Indeed (assuming the existence of oblivious transfer), the above $\Theta(1/\sqrt{r})$ lower bound does not hold in the standard model (where parties are) for $n < \text{loglog}\, r$ (see [9, 21, 24]).

1.2.2 Towards an Efficient Attack via Augmented Weak Martingales

The first step toward making the above attack efficient is *not* to base the X_i's on the transcript. Indeed, even given the first message T_1, computing $\mathbf{E}\left[\mathsf{out} \mid T_1\right]$ might involve inverting a one-way function. Our idea is to let $X^j_i = \mathbf{E}\left[\mathsf{out} \mid Z^j_{\leq i}\right]$; namely, the expected outcome given P^j's backup values. The immediate advantage is that the backup values are only bits. Thus, for instance, X^j_1 has only two possible values, and computing it from Z_1 can be done using one bit of non-uniform advice. Yet, for large values of i, the computation of X^j_i (depending on $Z^j_1, \ldots, Z^j_i$) might still be infeasible.

Here comes to help our new result for augmented weak martingales (Theorem 1.2). Let $f(Z^j_1, \ldots, Z^j_r) = \mathbf{E}\left[\mathsf{out} \mid Z^j_{\leq r}\right]$. By definition, it holds that $f(Z^j_1, \ldots, Z^j_r) = Z^j_r \in \{0,1\}$, and thus $\mathbf{E}\left[f(Z^j_1, \ldots, Z^j_r)\right] = 1/2$. Theorem 1.2 yields the existence of short (i.e., $\log r$) output, efficient function χ, such that for the Doob augmented weak martingales $X^j_i = \mathbf{E}\left[\mathsf{out} \mid Z^j_i, \chi(Z^j_{\leq i-1})\right]$,[3] it holds that (again, omitting absolute values and constant factors)

$$\Pr\left[\exists i \in [r] \colon X^j_i - X^j_{i-1} \geq 1/\sqrt{r}\right] \in \Omega(1) \tag{3}$$

So now X^j_i is only a function of $r \cdot \left|\text{Supp}(Z^j_i)\right| \cdot |\text{Im}(\chi)| \in O(r^2)$,[4] and thus can be computed efficiently. Namely, the martingale attack of [11] with respect to the above definition of X_i (i.e., aborting when seeing a gap), is now efficient. Similarly to [11], we would have an $\Omega(1/\sqrt{r})$ attack if

$$\Pr\left[\exists i \in [r] \colon \mathbf{E}\left[Z^{\bar{j}}_{i-1} \mid Z^j_i, \chi(Z^j_{\leq i-1})\right] - X^j_i \geq 1/2\sqrt{r}\right] \in \Omega(1) \tag{4}$$

The upper-bounds of [9, 21, 24], however, yield the latter might not hold, and generally, there is no way to exploit it for a different (efficient) attack. Fortunately, it turns out that for the case $n \geq r$, the suitable variant of the above inequality does hold, yielding that the above "martingale" attack goes through for this case. The case $n^k \geq r$ for $k \geq 2$ is significantly more complex, but still goes through. Details below.

[2] In more detail, assume for simplicity that P_0 sends the messages $T_1, T_3, \ldots$, and P_1 sends the messages $T_2, T_4, \ldots,$. Hence, for at least one party P_j, Equation (2) holds when limiting i to be a round in P_j is suppose to send the i^{th} message. The above attack is effective when mounted by this party.

[3] We omit X_{i-1} from the conditioning in the definition of X^j_i, since without loss of generality $\chi(Z_{\leq i-1})$ contains X^j_{i-1}.

[4] Actually, this requires considering a *rounded* version of X^j_i.

1.2.3 Efficient Attack for $n = r$

Let $(\mathsf{P}_1, \ldots, \mathsf{P}_n)$ be the parties of Π. For $j \in [n]$, let $Z_j^j \in \{0,1\}$ be the output (backup value) party P_j outputs if *all* parties but him abort right after the i^{th} round, and for $\mathcal{S} \subseteq [n]$ let $Z_i^{\mathcal{S}} = \frac{1}{|\mathcal{S}|} \cdot \sum_{s \in \mathcal{S}} Z_i^s$. For a subset $\mathcal{S} \subseteq [n]$, consider the sequence of augmented weak martingales $X_i^{\mathcal{S}} = \mathbf{E}\left[\mathsf{out} \mid Z_i^{\mathcal{S}}, \chi(Z_{\leq i-1}^{\mathcal{S}})\right]$, for χ being the function guaranteed by Theorem 1.2. As before, with constant probability $X_i^{\mathcal{S}} - X_{i-1}^{\mathcal{S}} \geq 1/\sqrt{r}$ for some $i \in [r]$. Hence, without loss of generality,

$$\Pr\left[\exists i \in [r] \colon X_i^{\mathcal{S}} - Z_{i-1}^{\mathcal{S}} \geq 1/2\sqrt{r}\right] \in \Omega(1) \tag{5}$$

A crucial observation, and the reason why considering number of parties that is *linear* in the round complexity is rewarding, is that with high probability over the choice of $\mathcal{S}$ of size $n/2$, it holds that

$$\forall i \in [r] \colon \quad Z_i^{\mathcal{S}} = Z_i^{\overline{\mathcal{S}}} \pm 1/3\sqrt{r} \tag{6}$$

Namely, $Z_i^{\mathcal{S}}$ is a good estimation for $Z_i^{\overline{\mathcal{S}}}$, for all rounds $i \in [r]$ *simultaneously*.[5]

Indeed, since $\mathcal{S}$ is chosen at random, $Z_i^{\mathcal{S}}$ $(= \frac{1}{|\mathcal{S}|} \cdot \sum_{s \in \mathcal{S}} Z_i^s)$ is a $1/3\sqrt{r}$ approximation of $Z_i^{[n]}$ and thus of $Z_i^{\overline{\mathcal{S}}}$. Fix such a good set $\mathcal{S}$. The following martingale attack biases the output of a random party P_h, for $h \leftarrow \overline{\mathcal{S}}$, towards one by $\Omega(1/\sqrt{r})$: in the i^{th} round, the attacker aborts all parties but P_h if $X_i^{\mathcal{S}} - Z_{i-1}^{\mathcal{S}} \geq 1/6\sqrt{r}$. Equations (5) and (6) implies that the above adversary biases the output of P_h towards one by $\Omega(1/\sqrt{r})$.

1.2.4 Efficient Attack for $n^k \geq r$ for $k \geq 2$ via Differentially Private Based Oblivious Sampling

We describe the attack for $n^2 \geq r$, and then briefly highlight the extension for $k \geq 3$.

A critical part of the above attack for $n = r$ (stated in (6)) is that for a random (and thus for some) subset $\mathcal{S} \subseteq [n]$ of size $n/2$, it holds that $Z_i^{\mathcal{S}}$ is an $O(1/\sqrt{r})$ approximation of $Z_i^{\overline{\mathcal{S}}}$. This might no longer be the case, however, if $n^2 = r$. Rather, we only guarantee that $Z_i^{\mathcal{S}}$ is an $O(1/\sqrt{n}) = O(1/\sqrt[4]{r})$ approximation of $Z_i^{\overline{\mathcal{S}}}$, which is a too rough approximation.

Our solution is to consider the *joint* backup values of *pairs* of parties, that is, the joint output of such pair given that all other parties abort. Considering the pairs' backup values, however, raises a new problem. The adversary can no longer examines the backup values of a random large subset $\mathcal{P} \subsetneq \binom{[n]}{2}$ of backup values, as we did in the case $n = r$, since with high probability *each* party in $[n]$ (and, in particular, the honest party) takes part in $\Theta(1/n)$ fraction of $\mathcal{P}$. So rather, we let the attacker examine the backup values of the pairs $\binom{\mathcal{S}}{2}$ for some subset $\mathcal{S} \subsetneq [n]$. We show that while (the average) of these backup values might not be a good approximation for the backup value of pairs that do contain the honest party, if this does not hold then we can employ a different type of attack using differentially private based oblivious sampling (Theorem 1.3). Details below.

For a pair $p = (j_1, j_2) \in \binom{[n]}{2}$, let $Z_j^p \in \{0,1\}$ be the joint output (backup value) of the parties P_{j_1} and P_{j_2}, if *all* parties but them abort right after the i^{th} round, and for $\mathcal{P} \subseteq \binom{n}{2}$, let $Z_i^{\mathcal{P}} = \frac{1}{|\mathcal{P}|} \cdot \sum_{p \in \mathcal{P}} Z_i^p$. For a subset $\mathcal{S} \subseteq [n]$, consider the sequence of augmented weak martingales $X_i^{\mathcal{S}} = \mathbf{E}\left[\mathsf{out} \mid X_{i-1}^{\mathcal{S}}, Z_i^{\binom{\mathcal{S}}{2}}, \chi(Z_{\leq i-1}^{\mathcal{S}})\right]$, for χ being the function guaranteed by Theorem 1.2. As

[5] Actually, this requires $n = r \log r$, but we ignore such log factors in this informal discussion.

before, with constant probability $X^{\mathcal{S}}_{i+1} - X^{\mathcal{S}}_i \geq 1/\sqrt{r}$ for some i. Assuming

$$Z_i^{\binom{\mathcal{S}}{2}} = Z_i^{\mathcal{S}\times\overline{\mathcal{S}}} \pm o(1/\sqrt{r}) \tag{7}$$

then, similar to the case of $n = r$, the following martingale attack biasses the output of a random party P_h, for $h \leftarrow \overline{\mathcal{S}}$, towards zero by $\Omega(1/\sqrt{r})$: in the i^{th} round, if $X^{\mathcal{S}}_i - X^{\mathcal{S}}_{i-1} > 1/\sqrt{r}$ the attacker aborts all parties but $(\mathsf{P}_h, \mathsf{P}_s)$ for a random $s \leftarrow \mathcal{S}$.

The differentially private based oblivious sampling attack. Unlike the case $n = r$, here Equation (7) might be false for any set $\mathcal{S}$. Fortunately, if that is the case, we can apply the following attack using the differentially private based oblivious sampling of Theorem 1.3. Assume for simplicity that

$$\Pr\left[\exists i \in [r] \colon Z_i^{\binom{\mathcal{S}}{2}} - Z_i^{\mathcal{S}\times\overline{\mathcal{S}}} > 1/\sqrt{r}\right] \in \Omega(1) \tag{8}$$

This calls for the following attack for biassing a random honest party P_h, for $h \leftarrow \mathcal{S}$, towards one. For $\mathcal{P} \in \left\{\binom{\mathcal{S}}{2}, \mathcal{S}\times\overline{\mathcal{S}}\right\}$, let $\mathcal{P} \setminus h$ stand for all pairs in $\mathcal{P}$ that do not include h. In the i^{th} round, the attacker checks whether $G_i = Z_i^{\binom{\mathcal{S}}{2}\setminus h} - Z_i^{(\mathcal{S}\times\overline{\mathcal{S}})\setminus h} > 1/\sqrt{r}$, if positive it aborts all parties but $(\mathsf{P}_h, \mathsf{P}_s)$ for a random $s \leftarrow \mathcal{S}$. It is not hard to get convinced that the attacker performs well if we have the guarantee that

$$G_i = G_i^h \pm o(1/\sqrt{r}) \tag{9}$$

for $G_i^h = Z_i^{\{h\}\times(\mathcal{S}\setminus\{h\})} - Z_i^{\{h\}\times\overline{\mathcal{S}}}$; namely, the backup values the attacker based its action upon approximate well the expected honest party output in case of abort. However, it can only be shown that

$$G_i = G_i^h \pm o(1/\sqrt{n}) = G_i^h \pm o(1/\sqrt[4]{r}) \tag{10}$$

Indeed if the above does not hold, then without loss of generality for some party $h' \in \mathcal{S}$ it holds that $Z_i^{\{h\}\times\overline{\mathcal{S}}} \neq Z_i^{\{h'\}\times\overline{\mathcal{S}}} \pm o(1/\sqrt[4]{r})$. But if this holds, a variant of the martingale attacked used for $n = r$ yields a $O(1/\sqrt{r})$ attack on a random party indexed in $\overline{\mathcal{S}}$.

So we need to find an attack that works only using the weaker guarantee of Equation (10). Fortunately, we are just in the setting of the differentially private based oblivious sampling theorem: Equation (8) yields that (with constant probability) $\max_i\{G_i\} \geq 1/\sqrt{r}$, and Equation (10) yields that $\left|G_i - G_i^h\right| < 1/\sqrt[4]{2r})$ for any $h \in \mathcal{S}$. Hence, Theorem 1.3 yields that for the differentially private variant of the above attack mounted on a random $H \leftarrow \mathcal{S}$, the expected value of G_J^H, for J being the aborting round, is at least $1/\sqrt{r} - (1/\sqrt[4]{2r})^2 > 1/4\sqrt{r}$, yielding a bias of this order on the output of P_H.

The case $n^k \geq r$ for $k \geq 3$. Assume for a start that $k = 3$ (i.e., $n^3 \geq r$). For such value of n, it holds that $1/\sqrt{n} = 1/\sqrt[6]{r} \gg 1/\sqrt[4]{r}$. Thus, the promise $G_i = G_i^h \pm o(1/\sqrt{n})$ does not suffice for the differentially private based attack to go through. Rather, we need to assume that $G_i = G_i^h \pm o(1/\sqrt[4]{r}) = G_i^h \pm o(1/n^{3/4})$. We show that if the latter does not hold, the attacker can fix a party and never abort it (i.e., we restrict the subset of all backup values to those containing

this party) we are essentially in the setting of $n^2 \geq r$. Namely, either we have differentially private based attack or the martingale attack (both with respect to the above fixing of a never aborting party).

For larger values of k, we iterate the above, fixing non-aborting parties one after the other, until one of the differentially private based attacks or the martingale attack go through.

1.3 Related Work

1.3.1 Coin Flipping

A coin-flipping protocol is δ-bias, if no efficient attacker (controlling all parties but one) can bias the honest party output by more than δ.

Upper bounds. Blum [8] presented a two-party two-round coin-flipping protocol with bias 1/4. Awerbuch et al. [5] presented an n-party r-round protocol with bias $O(n/\sqrt{r})$ (the two-party case appears also in Cleve [10]). In a surprising result, Moran, Naor, and Segev [23] presented a two-party r-round coin-flipping protocol with bias $O(1/r)$. Haitner and Tsfadia [20] almost resolved the case of three parties, constructing a three-party coin-flipping protocol with bias $O(\text{polylog}(r)/r)$. Buchbinder et al. [9] constructed an n-party r-round coin-flipping protocol with bias $\widetilde{O}(n^3 2^n / r^{\frac{1}{2}+\frac{1}{2^{n-1}-2}})$. In particular, their four-party coin-flipping protocol the bias is $\widetilde{O}(1/r^{2/3})$ and for $n = \log\log r$ their protocol has bias smaller than [5].

For the case where less than 2/3 of the parties are corrupt, Beimel et al. [7] have constructed an n-party r-round coin-flipping protocol with bias $2^{2^k}/r$, tolerating up to $t = (n+k)/2$ corrupt parties. Alon and Omri [1] constructed an n-party r-round coin-flipping protocol with bias $\widetilde{O}(2^{2^n}/r)$, tolerating up to t corrupted parties, for constant n and $t < 3n/4$.

Lower bounds. Cleve [10] has proved that for every r-round two-party coin-flipping protocol there exists is an efficient adversary that can bias the output by $\Omega(1/r)$. Cleve and Impagliazzo [11] have proved that even in the *fail-stop model*, for every r-round two-party coin-flipping protocol there exists an unbounded adversary that can bias the output by $\Omega(1/\sqrt{r})$. The same bound also holds in the commitment-fail-stop model (with unbounded adversaries.). Both bounds extend to multi-party protocol (with no honest majority) via a simple reduction.

Dachman-Soled et al. [12], Dachman-Soled et al. [13] have studied the minimal assumptions required to achieve an optimal bias of $O(1/r)$ for two-party protocols. [12] have shown that any fully black-box construction of optimally-fair coin-flipping protocols based on one-way functions with r-bit input and output needs $\Omega(r/\log r)$ rounds. [13] have shown that there is no fully black-box and function *oblivious* construction of optimally-fair coin-flipping protocols from one-way functions (a protocol is function oblivious if the outcome of the protocol is independent of the choice of the one-way function used in the protocol). Both papers use the result of [11] mentioned above.

1.3.2 $1/p$-Secure Protocols

Cleve [10] result implies that for many functions fully-secure computation without an honest majority is not possible. Gordon and Katz [18] suggested the notion of $1/p$-secure computation to bypass this impossibility result. Very informally, a protocol is $1/p$-secure if every poly-time adversary can

harm the protocol with probability at most $1/p$ (e.g., with probability $1/p$ the adversary can learn the inputs of honest parties, get the output and prevent the honest parties from getting the output, or bias the output). Gordon and Katz [18] constructed for every polynomial $p(\kappa)$ (where κ is the security parameter) an efficient two-party $1/p(\kappa)$-secure protocol for computing a function f, provided that the size of the domain of at least one party in f or the size of the range of f is bounded by a polynomial. Beimel, Lindell, Omri, and Orlov [6] generalized this result to multi-party protocols when the number of parties is constant – for every function f with $O(1)$ inputs such that the domain of each party (or the size of the range of f) is bounded by a polynomial and for every polynomial $p(\kappa)$, they presented an efficient $1/p(\kappa)$-secure protocol for computing the function.

Gordon and Katz [18] and Beimel et al. [6] also provided impossibility results explaining why their protocols require bounding the size of the domain or range of the functions. Specifically, Gordon and Katz [18] described a two-party function whose size of domain of each party and size of range is $\kappa^{\omega(1)}$ such that this function cannot be computed by any poly-round protocol achieving 1/3-security. Beimel et al. [6] used this result to construct a function $f\colon \{0,1\}^{\omega(\log n)} \to \kappa^{\omega(1)}$ (i.e., a function with $\omega(\log n)$ parties where the domain of each party is Boolean) such that this function cannot be computed by any poly-round protocol achieving 1/3-security. They also showed the same impossibility result for a function with $\omega(1)$ parties where the domain of each party is bounded by a polynomial is the security parameter. We emphasize that these impossibility results do not apply to coin-flipping protocols, where the parties do not have inputs.

1.3.3 Complete Fairness Without Honest Majority

Cleve [10] result was interpreted as saying that non-trivial functions cannot be computed with complete fairness without an honest majority. In a surprising result, Gordon, Hazay, Katz, and Lindell [19] have shown that the millionaire problem with a polynomial size domain and other interesting functions can be computed with complete fairness in the two-party setting. The two-party functions that can be computed with complete fairness were further studied in [3, 2, 22, 4]; in particular, Asharov et al. [4] characterized the Boolean functions that can be computed with complete fairness. Gordon and Katz [17] have studied complete fairness in the multi-party case and constructed completely-fair protocols for non-trivial functions in this setting.

1.3.4 Differential Privacy

Differential privacy, introduced by Dwork et al. [15], provides a provable guarantee of privacy for data of individuals. Assume there is a database containing private information of individuals and there is an algorithm computing some function of the database. We say that such randomized algorithm is differentially private if changing the data of one individual has small affect on the output of the algorithm. For example, if, for a database D, a function $f(D)$ returns a numerical value in $[0,1]$, then an algorithm returning $f(D) + \mathit{noise}$, where *noise* is distributed according to the Laplace distribution (with suitable parameters), is a differentially private algorithm. Since the introduction of differential privacy in 2006, many algorithms satisfying differential privacy were introduced, see, e.g., Dwork and Roth [14]. In this work we use differential privacy (i.e., Laplace noise) not for protecting privacy, but rather to provide oblivious sampling. This is similar in spirit to the usage of differential privacy, by Dwork et al. [16], to enable adaptive queries to a database.

Paper Organization

Basic definitions and notation used through the paper, are given in Section 2. We also prove therein some useful inequalities used by the different sections. The proof of the main theorem is given in Section 3. The proof uses our result for augmented week martingales, proved in Section 4, and oblivious sampling, proved in Sections 4 and 5 respectively.

In this version, we state and prove the different results for *non-uniform* polynomial-time algorithms (i.e., polynomial-size circuits).

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values, and boldface for vectors. All logarithms considered here are in base two. For a vector $\mathbf{v}$, we denote its i^{th} entry by $\mathbf{v}_i$ or $\mathbf{v}[i]$. For $a \in \mathbb{R}$ and $b \geq 0$, let $a \pm b$ stand for the interval $[a-b, a+b]$. Given sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$ and k-input function f, let $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) := \{f(x_1, \ldots, x_j) \colon x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) \colon x \in [.9, 1.1]\}$. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$. Given a vector $\mathbf{v} \in \{0,1\}^*$, let $w(\mathbf{v}) := \sum_{i \in [|\mathbf{v}|]} \mathbf{v}_i$. For $x, \delta \in [0,1]$ let $\mathsf{rnd}_\delta(x) = k\delta$, for $k \in \mathbb{Z}$ being the largest number with $k\delta \leq x$. For a function $f \colon \mathcal{A} \mapsto \mathcal{B}$, let $\mathrm{Im}(f) = \{f(a) \colon a \in \mathcal{A}\}$.

Let poly denote the set of all polynomials, let PPT stand for probabilistic polynomial time, let PPTM denote a PPT algorithm (Turing machine) and let $\text{PPTM}^{\mathsf{NU}}$ stands for a *non-uniform* PPTM. A function $\nu \colon \mathbb{N} \to [0,1]$ is *negligible*, denoted $\nu(n) = \mathrm{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in \mathrm{poly}$ and large enough n.

2.2 Coin-Flipping Protocols

Since the focus of this paper is showing the non-existence of coin-flipping protocols with small bias, we will only focus on the correctness and bias of such protocols. See [21] for a complete definition of such protocols.

Definition 2.1 (correct coin-flipping protocols)**.** *A multi-party protocol is a* correct coin-flipping protocol*, if*

- *When interacting with an efficient adversary controlling a subset of the parties, the honest parties* always *output the same bit, and*
- *The common output in a random* honest *execution of the protocol is a uniform bit.*

Definition 2.2 (Biassing coin-flipping protocols)**.** *An adversary* A *controlling a strict subsets of the parties of a correct coin-flipping protocol* biases *its output by $\delta \in [1/2, 1]$, if when interacting with the parties controlled by* A*, the remaining honest parties output some a priory fixed bit $b \in \{0,1\}$ with probability $\frac{1}{2} + \delta$.*

Such an adversary is called fail stop*, if the parties in its control honestly follow the prescribed protocol, but might abort prematurely. The adversary is a rushing adversary, that is, in each round, first the honest parties send their messages, then the adversary might instruct some of the parties to abort (that is, send a special "abort" message to all other parties), and finally, all corrupt parties that have not aborted send their messages.*

2.3 Basic Probability Facts

Given a distribution D, we write $x \leftarrow D$ to indicate that x is selected according to D. Similarly, given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution on $\mathcal{S}$. Let D be a distribution over a finite set $\mathcal{U}$, for $u \in \mathcal{U}$, denote $D(u) = \Pr_{X \leftarrow D}[X = u]$ and for $\mathcal{S} \subseteq \mathcal{U}$ denote $D(\mathcal{S}) = \Pr_{X \leftarrow D}[X \in \mathcal{S}]$. Let the support of D, denoted $\mathrm{Supp}(D)$, be defined as $\{u \in \mathcal{U} : D(u) > 0\}$. The *statistical distance* between two distributions P and Q over a finite set $\mathcal{U}$, denoted as $\mathrm{SD}(P, Q)$, is defined as $\max_{\mathcal{S} \subseteq \mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$.

2.3.1 The Laplace Distribution

Definition 2.3. *The Laplace distribution with parameter $\lambda \in \mathbb{R}^+$, denoted $\mathsf{Lap}(\lambda)$, is defined by the density function $f(x) = \exp(-|x|/\lambda)/2\lambda$.*

The following facts easily follow from the definition of the Laplace distribution.

Fact 2.4. *For every $x \in \mathbb{R}$, it holds that*

$$\begin{aligned} \Pr[\mathsf{Lap}(\lambda) \geq \lambda |x|] &= \frac{1}{2} \cdot \exp(-|x|), \\ \Pr[\mathsf{Lap}(\lambda) \geq -\lambda |x|] &= 1 - \frac{1}{2} \cdot \exp(-|x|). \end{aligned}$$

Fact 2.5. *Let $\gamma, \gamma' \in \mathbb{R}$ and $\lambda \in \mathbb{R}^+$. Let $p = \Pr[\mathsf{Lap}(\lambda) \geq \lambda\gamma]$ and $p' = \Pr[\mathsf{Lap}(\lambda) \geq \lambda\gamma']$. If $|\varepsilon = \gamma' - \gamma| \leq 1$, then $p/p' \in 1 \pm 5\varepsilon$.*

For completeness, the proof of Fact 2.5 is given in Appendix A.

2.3.2 Useful Observations about Iterated Bernoulli Trials

The next lemma bounds the statistical distance between the first success for two experiments of r independent Bernoulli trials satisfying a certain notion of closeness.

Lemma 2.6. *Consider two iterative sequences, each of r independent Bernoulli trials. Let $p_i, p'_i \in [0, 1]$ denote the success probability of the i^{th} trial of the first and second sequence, respectively. Assume that $p_r = p'_r = 1$. For $i \in [r]$, let $q_i = p_i \cdot \prod_{j<i}(1 - p_j)$ and $q'_i = p'_i \cdot \prod_{j<i}(1 - p'_j)$. Let ε be such that for all $i \in [r]$, it holds that $\frac{p_i}{p'_i}, \frac{p'_i}{p_i}, \frac{(1-p'_i)}{(1-p_i)}, \frac{(1-p_i)}{(1-p'_i)} \in (1 \pm \varepsilon)$. Then, $\sum_{i=1}^{r-1} |q_i - q'_i| \leq 4\varepsilon(1 - q_r)$.*

The proof of Lemma 2.6 is given in Appendix A (see Lemma A.4).

The following fact is a variant of [11, Lemma 6]. In loose terms, it bounds the probability that the sum of the expectation of r events exceeds a certain quantity while none of those events occurred.

Fact 2.7. *Let $A_1 \ldots A_r$ be a sequence of random variables. Let D_i denote an event and suppose that A_i fully determines $\overline{D}_1 \wedge \ldots \wedge \overline{D}_i$. Further define $C_i = \mathbf{E}[D_i \mid A_{i-1}]$. It holds that, for every $\gamma \geq 0$,*

$$\Pr\left[\left(\sum_{i=1}^{r} C_i \geq \gamma\right) \wedge \overline{D}_1 \wedge \ldots \wedge \overline{D}_r\right] \leq e^{-\gamma} \ .$$

Fact 2.8 (Hoeffding's inequality)**.** *Let* $\mathcal{X} = \{x_i \in \{0,1\}\}_{i=1}^n$ *and* $\mu = \frac{1}{n} \cdot \sum_{i=1}^n x_i$*. Let* $E \leftarrow \binom{[n]}{n/2}$ *i.e. E denotes a random subset of* $[n]$ *of size* $n/2$*. For any* $\varepsilon \geq 0$*, it holds that*

$$\Pr\left[\left|\mu - \frac{2}{n} \cdot \sum_{\ell \in E} x_i\right| \geq \varepsilon/\sqrt{n}\right] \leq 2\exp(-\varepsilon^2) \ .$$

2.3.3 Useful Observations about Conditional Expectation

The proofs of the following facts are given in Appendix A.

Fact 2.9. *For* $\delta \in \mathbb{R}$ *and random variables A, B and C, if* $\mathbf{E}[A \mid B, C] \in \pm\delta$*, then* $\mathbf{E}[A \mid B] \in \pm\delta$*.*

Fact 2.10. *For random variables A, B and function f, it holds that*

$$\mathbf{E}[\mathbf{E}[A \mid B] \mid f(B)] = \mathbf{E}[A \mid f(B)] \ .$$

Fact 2.11. *For random variables A, B, C and a function f, it holds that*

$$\mathbf{E}[\mathbf{E}[A \mid B, C] \mid \mathbf{E}[A \mid B], f(B)] = \mathbf{E}[A \mid B] \ .$$

Fact 2.12. *Let A, B, and C be random variables such that* $A, B \in [0,1]$*. If* $\mathbf{E}[A \mid B, C] = B$ *then*

$$\mathbf{E}[A \mid \mathsf{rnd}_\delta(B), C] \in \mathsf{rnd}_\delta(B) \pm \delta \ .$$

2.4 Martingales

In this section we define weaker variants of martingales. We show that these weaker variants satisfy a variant of Azuma's inequality.

Definition 2.13 (δ-martingales)**.** *Let* $X_0, \ldots, X_r$ *be a sequence of random variables. We say that the sequence is a* δ-strong *martingale sequence if* $\mathbf{E}[X_{i+1} \mid X_{\leq i} = x_{\leq i}] \in x_i \pm \delta$ *for every* $i \in [r-1]$*. We say that the sequence is a* δ-weak *martingale sequence if* $\mathbf{E}[X_{i+1} \mid X_i = x_i] \in x_j \pm \delta$ *for every* $i \in [r-1]$*. If* $\delta = 0$*, the above are just called* strong *and* weak *martingale sequence respectively.*

Speaking loosely, a sequence is a strong martingale if the expectation of the next point conditioned on the entire history is exactly the last observed point. Analogously, a sequence is a weak martingale if the expectation of the next point conditioned on the previous point is equal to the previous point.

Definition 2.14 (δ-martingale difference sequence)**.** *Let* $X_0, \ldots, X_r$ *be a* δ-strong *or* δ-weak *martingale sequence and define* $Y_i = X_i - X_{i-1}$*. The sequence* $Y_1 \ldots Y_r$ *is referred to as the* δ-strong *or* δ-weak *martingale difference sequence.*

By Definitions 2.13 and 2.14, it follows immediately that a sequence $Y_1 \ldots Y_r$ is a δ-strong martingale difference if and only if $\mathbf{E}[Y_i \mid Y_1, \ldots, Y_{i-1}] \in \pm\delta$, and that a sequence $Y_1 \ldots Y_r$ is a δ-weak martingale difference if and only if $\mathbf{E}\left[Y_i \mid \sum_{\ell<i} Y_\ell\right] \in \pm\delta$.

Theorem 2.15 (Azuma's inequality for submartingales)**.** *Let* $Z_0, \ldots, Z_r$ *be a sequence of random variables. Assume that* $|Z_i - Z_{i-1}| \leq s$ *and* $\mathbf{E}[Z_i - Z_{i-1} \mid Z_{j<i}] \leq 0$*, for every* $i \in \{1, \ldots, r\}$*. Then for every* $\lambda > 0$

$$\Pr\left[Z_r - Z_0 \geq \lambda s\sqrt{r}\right] \leq \exp(-\lambda^2/2) \ .$$

Theorem 2.16 (Azuma's inequality for δ-martingales)**.** *Let $X_0, \ldots, X_r$ be a sequence of random variables. Assume that $|X_i - X_{i-1}| \leq s$, for every $i \in \{1, \ldots, r\}$. If $X_1 \ldots X_r$ is a δ-*strong *or δ-*weak *martingale then for every $\lambda > 0$*

$$\Pr\left[|X_r - X_0| \geq \lambda(s+\delta)\sqrt{r} + r \cdot \delta\right] \leq 2\exp(-\lambda^2/2) \ .$$

Proof. An immediate consequence of Lemmas 2.17 and 2.18. □

Lemma 2.17. *For every δ-strong martingale $X_0 \ldots X_r$ satisfying $|X_i - X_{i-1}| \leq s$ for every $i \in [r]$, it holds that for every $\lambda > 0$*

$$\Pr\left[\ |X_r - X_0| \geq \lambda(s+\delta)\sqrt{r} + r \cdot \delta\right] \leq 2\exp(-\lambda^2/2) \ . \tag{11}$$

Proof. Let $X_1, \ldots, X_r$ be a δ-strong martingale and let $Y_i = X_i - X_{i-1}$. Thus, $|Y_i| \leq s$, for every $i \in [r]$. By the definition of the δ-strong martingale, $\mathbf{E}[Y_i - \delta \mid Y_{j<i}] \leq 0$ and $\mathbf{E}[Y_i + \delta \mid Y_{j<i}] \geq 0$. Lemma 2.17 follows from applying Theorem 2.15 to the sequences $(X_0 + r\delta, X_1 + (r-1)\delta, \ldots, X_{r-1} + \delta, X_r)$ and $(-X_0, -X_1 - \delta, \ldots, -X_{r-1} - (r-1)\delta, -X_r - r\delta)$. □

Lemma 2.18. *For every δ-weak martingale $X_0 \ldots X_r$, there exists a δ-strong martingale $Z_1, \ldots, Z_r$ such that (X_i, X_{i-1}) and (Z_i, Z_{i-1}) are identically distributed, for every $i \in [r]$.*

Proof. Let $X_1, \ldots, X_r$ be a δ-weak martingale and let $Y_i = X_i - X_{i-1}$ denote the difference sequence. We will construct a sequence of random variables that satisfies the strong variant of the martingale definition, and we will show that it is point-wise identically distributed to the sequence $X_1, \ldots, X_r$. Inductively, $Z_0 = X_0$ and $Z_i = Z_{i-1} + Y'_i$ where Y'_i is the random variable that returns y with probability $\Pr[Y_i = y \mid Z_{i-1} = X_{i-1}]$.

Claim 2.19. *The sequence $Z_1, \ldots, Z_r$ is a δ-strong martingale.*

Proof. We compute the expectation of Z_i conditioned on $Z_{i-1}, \ldots, Z_0$ to verify that it satisfies the strong variant of Definition 2.13.

$$\begin{aligned}
\mathbf{E}[Z_i \mid Z_{i-1}, \ldots, Z_0] &= \mathbf{E}\left[Z_{i-1} + Y'_i \mid Z_{i-1}, \ldots, Z_0\right] \\
&= \mathbf{E}\left[Z_{i-1} + Y'_i \mid Z_{i-1}, \ldots, Z_0\right] \\
&= Z_{i-1} + \mathbf{E}\left[Y'_i \mid Z_{i-1}, \ldots, Z_0\right].
\end{aligned}$$

It remains to show that $\mathbf{E}[Y'_i \mid Z_{i-1}, \ldots, Z_0] \in \pm\delta$. Intuitively, this is true because Y'_i is independent of the history of the Z's, and it is sampled according to Y_i which satisfies $\mathbf{E}[Y_i \mid X_{i-1}] \in \pm\delta$. So,

$$\mathbf{E}\left[Y'_i \mid Z_{i-1}, \ldots, Z_0\right] = \mathbf{E}\left[Y'_i \mid Z_{i-1}\right]$$

and

$$\begin{aligned}
\mathbf{E}\left[Y'_i \mid Z_{i-1} = w\right] &= \sum_y y \cdot \Pr\left[Y'_i = y \mid Z_{i-1} = w\right] \\
&= \sum_y y \cdot \Pr[Y_i = y \mid X_{i-1} = w] = \mathbf{E}[Y_i \mid X_{i-1} = w] \in \pm\delta.
\end{aligned}$$

□

Claim 2.20. *(X_i, X_{i-1}) and (Z_i, Z_{i-1}) are identically distributed, for every $i \in [r]$.*

Proof. We prove the statement by induction. Obviously $(X_0, X_1) = (Z_0, Z_1)$. Next, assume that (X_i, X_{i-1}) and (Z_i, Z_{i-1}) are identically distributed, i.e. for every $x \in \mathrm{supp}(X_{i-1})$, $\Pr[X_{i-1} = x] = \Pr[Z_{i-1} = x]$. To conclude, observe that

$$\begin{aligned}
\Pr\left[(Z_{i+1}, Z_i) = (x, x')\right] &= \Pr\left[Z_{i-1} + Y_i' = x \wedge Z_i = x'\right] \\
&= \Pr\left[Y_i' = x - x' \wedge Z_i = x'\right] \\
&= \Pr\left[Y_i' = x - x' \mid Z_i = x'\right] \cdot \Pr\left[Z_i = x'\right] \\
&= \Pr\left[Y_i = x - x' \mid X_i = x'\right] \cdot \Pr\left[X_i = x'\right] \\
&= \Pr\left[Y_i = x - x' \wedge X_i = x'\right] = \Pr\left[X_{i+1} = x \wedge X_i = x'\right].
\end{aligned}$$

□
□

3 Biasing Coin-Flipping Protocols

In this section we prove our main result, an almost optimal attack on many-party coin-flipping protocols.

Theorem 3.1. *There exists a fails-stop adversary A such that the following holds. Let Π be a correct n-party r-round coin-flipping protocol, and let $k \in \mathbb{N}$ be the smallest integer such that $\binom{n}{k} \geq r\log(r)^{2k}$. Then, there exists a party P in Π and a string $\mathsf{adv} \in \{0,1\}^*$ such that $\mathsf{A}^{\Pi}(\mathsf{adv})$ controlling all parties but P biases the output of P by $O(1/\sqrt{r}\log(r)^k)$. The running time of A^{Π} is polynomial in the running time of Π and n^k, and it uses only oracle access to Π's next-message function.*

Remark 3.2 (Interesting choice of parameters)**.** *Note that $\sqrt{n} \geq 2\log(r)^2$ implies $\binom{n}{\sqrt{n}} \geq \sqrt{n}^{\sqrt{n}} \geq 2^{\sqrt{n}}\log(r)^{2\sqrt{n}} \geq r\log(r)^{2\sqrt{n}}$, and therefore there exists $k \in \{1, \ldots, \sqrt{n}\}$ satisfying the hypothesis of the theorem. On the other hand, if $\sqrt{n} < 2\log(r)^2$, then it is easy to see that either such k does not exist, or $\log(r)^k \geq \sqrt{r}$ and in this case Cleve [10]'s bound overtakes and our theorem is trivial.*

Proving Theorem 3.1 The proof given below follows the high-level description given in the introduction. Recall that a backup value associated with a subset of parties with respect to a given round of a protocol execution, is the common output these parties would output if all other parties prematurely abort in this round round. More formally,

Notation 3.3. *We identify the set $[n]$ with the parties of the n-party protocol in consideration. We refer to subset of parties (i.e., subset of $[n]$) as* tuples*, and denote sets of such tuples using "blackboard bold" (e.g., $\mathbb{S}$) rather than calligraphic. For a tuple subset $\mathbb{S} \subseteq \binom{[n]}{k}$ and $h \in [n]$, let $\mathbb{S}(h) = \{\mathcal{U} \in \mathbb{S} \colon h \in \mathcal{U}\}$ and $\mathbb{S} \setminus h = \mathbb{S} \setminus \mathbb{S}(h)$.*

Definition 3.4 (Backup values)**.** *The following definitions are with respect to a fixed honest execution of an n-party, r-round correct protocol (determined by the parties' random coins). The i^{th}* round backup value *of a subset of parties $\mathcal{U} \subseteq [n]$ at round $i \in [r]$, denoted $\mathsf{Bckp}(\mathcal{U}, i)$, is defined as the common output the parties in u would output, if all other parties abort in the i^{th} round (set to $\perp$ if the execution has not reached this round with all parties of $\mathcal{U}$ alive). The* average backup value *of a tuples subset of $\mathbb{S}$, is defined by $\mathsf{AvgBckp}(\mathbb{S}, i) = \frac{1}{|\mathbb{S}|}\sum_{\mathcal{U}\in\mathbb{S}} \mathsf{Bckp}(\mathcal{U}, i)$.*

Back to the informal proof-sketch. For a party-subset $\mathcal{S} \subseteq [n]$, consider the backup value of the tuples in $\mathbb{S}_1 = \mathcal{S}^k$. That is, the random variables $Y_1^{\mathbb{S}_1}, \ldots, Y_r^{\mathbb{S}_1}$, denoting the value of $\mathsf{AvgBckp}(\mathbb{S}_1, i)$ in a random execution of Π. Let $X_0 \ldots, X_r$ be the Doob augmented weak martingales of this sequence. In Section 4, we show that with constant probability this martingale sequence has an $1/\sqrt{r}$ gap between two consecutive variables. Such a gap would enable an $1/\sqrt{r}$ attack, unless the sequence $Y_1^{\mathbb{S}_2}, \ldots, Y_r^{\mathbb{S}_2}$ for $\mathbb{S}_1 = \mathcal{S}^{k-1} \times \overline{\mathcal{S}}$, and the above sequence $Y_1^{\mathbb{S}_1}, \ldots, Y_r^{\mathbb{S}_1}$ are *non similar*: there is a $1/\sqrt{r}$ gap between $Y_i^{\mathbb{S}_2}$ and $Y_i^{\mathbb{S}_2}$ is some round i. If the latter holds, however, we can try and exploit this non-similarity by applying the oblivious sampling attack described in Section 5. For the latter attack to go through we need that for every two parties $h, h' \in [n]$, the restriction of the above sequence to h and h', defined by $Y_1^{\mathbb{S}_1(h)}, \ldots, Y_r^{\mathbb{S}_1(h)}$ and $Y_1^{\mathbb{S}_1(h')}, \ldots, Y_r^{\mathbb{S}_1(h')}$ are similar (and the same for $\mathbb{S}_2$). Furthermore, if one such pair of restriction is non similar, we can try to apply the oblivious sampling attack with the restricted sequences, and so forth.

This iterative process ends up by finding a non-similar pair of of tuple-sets such that every restriction is similar, and then we can apply the oblivious sampling attack. Or, the non-similar pair we find consists of tuples in which all-but-one parties are fixed, and in this case we can apply a simple attack that we call the *singletons attack*. We refer to the "level" where the process stops as the *nugget* of Π.

The actual proof is significantly more complicated as we have to use a different similarity measure for every level, and to make sure the set of restricted tuples are of the right size.

We formally prove the theorem using the following four lemmas, proved in Sections 3.1 to 3.4. Lemma 3.7 state that any protocol has a nugget (formally defined in Definition 3.6), where Lemmas 3.8 to 3.10 states that there is an effective attack, for all possible values of the nugget.

Notation 3.5. *Let* $\mathsf{coef}_n(k,\ell) = \frac{(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+\ell)}{(k-1)\cdot(k-2)\ldots\cdot\ell}$*, letting* $\mathsf{coef}_n(k,k) = 1$*. For* $r \in \mathbb{N}$*, let* $\mathcal{R}(r) = \{1, 1+1/r, 1+2/r, 1+3/r \ldots, r\}$.

Definition 3.6 (The Nugget)**.** *Let* Π *be an* n*-party* r*-round coin-flipping protocol, and let* $k \in \mathbb{N}$ *be the smallest integer such that* $\binom{n}{k} \geq r\log(r)^{2k}$*. Index* $k^* \in [k+1]$ *is a* nugget *for* Π*, if there exists* $\rho^* \in \mathcal{R}(r)$*, set* $\mathcal{H} \subseteq [n]$ *and tuple sets* $\mathbb{S}_1, \mathbb{S}_0 \subseteq \binom{n}{k}$ *such that the following holds.*

For a tuple-set $\mathbb{S} \subseteq 2^{[n]}$ *and* $i \in [r]$*, let* $Y_i^{\mathbb{S}}$ *denote the value of* $\mathsf{AvgBckp}(\mathbb{S}, i)$ *in a random execution of* Π*. The following holds according to the value of* k^**:*

$k^* = 1$**:**

1. $\Pr\left[\max_{i\in[r]}\left|Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0}\right| \geq \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*)^{1/2}}{(64\log(r))^{k-k^*}}\right] \geq \frac{1}{2\rho^*\log(r)} \cdot \frac{64^{-k+k^*}}{\mathsf{coef}_n(k,k^*)^{1/2}}$.
2. $\mathcal{H} \geq n/3$, $|\mathbb{S}_1| = |\mathbb{S}_0| = |\mathcal{H}|$*, and* $|\mathbb{S}_z(h)| = 1$ *for every* $h \in \mathcal{H}$ *and* $z \in \{0,1\}$.

$k^* \in \{2, \ldots, k\}$**:**

1. *Same as Item 1 for* $k^* = 1$.
2. *For every* $h, h' \in \mathcal{H}$*,* $z, z' \in \{0,1\}$*,* $\mathcal{U}' \in \mathbb{S}_z$ *and* $\rho \in \mathcal{R}(r)$*:*
   (a) $\Pr\left[\max_{i\in[r]}\left|Y_i^{\mathbb{S}_z(h)} - Y_i^{\mathbb{S}_z(h')}\right| \geq \frac{\rho}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*-1)^{1/2}}{(64\log(r))^{k-k^*+1}}\right] \leq \frac{1}{2\rho\log(r)} \cdot \frac{64^{-k+k^*-1}}{\mathsf{coef}_n(k,k^*-1)^{1/2}}$.
   (b) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h' \in \mathcal{U}] \leq \frac{1}{2}$.
   (c) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_{z'}}[h \in \mathcal{U}]$.

(d) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h\notin\mathcal{U}]/\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h\in\mathcal{U}]\geq\frac{1}{4}\cdot\frac{n-k+k^*-1}{k^*-1}$.
(e) $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}_z(h)}[\mathcal{U}=\mathcal{U}']=\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[\mathcal{U}=\mathcal{U}']$

$k^*=k+1$**:**

1. $\mathbb{S}_1(h)=\emptyset$ *for every* $h\in\mathcal{H}$.
2. $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}_0(h)}[\mathcal{U}=\mathcal{U}']=\Pr_{\mathcal{U}\leftarrow\mathbb{S}_0}[\mathcal{U}=\mathcal{U}']$ *for every* $\mathcal{U}'\in\mathbb{S}_0$.
3. $\Pr\left[\max_{i\in[r]}\left|Y_i^{\mathbb{S}_0}-Y_i^{\mathbb{S}_1}\right|\geq\frac{\rho}{256\sqrt{r}}\right]\leq\frac{1}{2\rho\log(r)}$ *for every* $\rho\in\mathcal{R}(r)$.

Lemma 3.7. *Let* Π *be an* n*-party* r*-round coin-flipping protocol, then* Π *has a nugget.*

Lemma 3.8. *There exists a fails-stop adversary* A *such that the following holds. Let* Π *be a correct* n*-party* r*-round coin-flipping protocol, and let* $k\in\mathbb{N}$ *be the smallest integer such that* $\binom{n}{k}\geq r\log(r)^{2k}$.

Suppose Π *admits a nugget* $k^*=k+1$*, then exists party* $h\in[n]$ *and a string* adv *such that* $\mathsf{A}^{\Pi}(\mathsf{adv})$ *controlling all parties but* h *biases the output of* h *by* $O(1/\sqrt{r}\log(r)^{k-k^*+1})$*. The running time of* A *is polynomial in the running time of* Π *and* n^k*, and it uses only oracle access to* Π*'s next-message function.*

Lemma 3.9. *Same as Lemma 3.8 with respect to* $k^*\in\{2,\ldots,k\}$.

Lemma 3.10. *Same as Lemma 3.8 with respect to* $k^*=1$.

Proof of Theorem 3.1. immediately follows from Lemmas 3.7, 3.11, 3.17 and 3.20. □

In the following we assume without loss of generality that r is larger than some constant to be determined by the analysis. This latest assumption does not incur any loss of generality, and we use it to make sure that the term $1/\sqrt{r}\log(r)^{k-k^*+1}$ dominates over other terms.

3.1 The Martingale Attack

Lemma 3.11 (Restatement of Lemma 3.8)**.** *There exists a fails-stop adversary* A *such that the following holds. Let* Π *be a correct* n*-party* r*-round coin-flipping protocol, and let* $k\in\mathbb{N}$ *be the smallest integer such that* $\binom{n}{k}\geq r\log(r)^{2k}$*. Suppose there exist tuple sets* $\mathbb{S},\mathbb{S}'\subseteq\binom{[n]}{k}$ *and party set* $\mathcal{H}\subseteq[n]$*, satisfying*

- $\mathbb{S}(h)=\emptyset$ *for every* $h\in\mathcal{H}$*, letting* $\mathbb{S}(h)$ *be according to Notation 3.3.*
- *For every* $\mathcal{U}'\in\mathbb{S}'$, $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}'(h)}[\mathcal{U}=\mathcal{U}']=\Pr_{\mathcal{U}\leftarrow\mathbb{S}'}[\mathcal{U}=\mathcal{U}']$.
- $\Pr\left[\max_i\left|Y_i^{\mathbb{S}}-Y_i^{\mathbb{S}'}\right|\geq\frac{\rho}{256\sqrt{r}}\right]\leq\frac{1}{2\rho\log(r)}$*, for every* $\rho\in\{1,1+1/r,\ldots,r\}$*, letting* $Y_i^{\mathbb{S}}=Y_i^{\mathbb{S}}(\Pi)$ *be according to Definition 3.4.*

Then there exists $h\in\mathcal{H}$ *and as a string advice* adv *such that* $\mathsf{A}^{\Pi}(\mathsf{adv})$ *corrupting all parties but* h*, biases the output of* h *by* $O(1/\sqrt{r})$.

Furthermore, the running time of $\mathsf{A}^{\Pi}(\mathsf{adv})$ *is polynomial in the running time of* Π *and* n^k*, and only uses oracle access to* Π*'s next-message function.*

3.1.1 The Game-Value Sequence

The cornerstone of the so called martingale attack is that, at every round, the adversary computes the expected outcome of the protocol, dubbed the *game-value* and denoted X_i for round i. Then, she compares this value to the backup value at hand, and decides to abort depending on whether the backup value deviates from the expected outcome of the protocol in a significant way. Next, we formally define the game-value sequence and follow up with a discussion regarding some of its properties.

Let $Z = (Z_2, \ldots, Z_r)$ for $Z_i = (Y_i^{\mathbb{S}}, Y_{i-1}^{\mathbb{S}})$, and for $z = ((y_2, y_1), \ldots, (y_r, y_{r-1})) \in \mathrm{Supp}(Z)$ let $f(z) = y_r$. Define $g : [0,1]^3 \times \{0,1\} \mapsto \{0,1\}$ by

$$g(x, y, y', \mathsf{aux}) = \begin{cases} \mathsf{aux} & \text{if } |y - x| < 1/64\sqrt{r} \vee |y' - x| < 1/64\sqrt{r}, \\ 0 & \text{otherwise;} \end{cases} \tag{12}$$

By Theorem 4.3, for every $\delta \leq 1/100r$, there exists a $(\log(r) + 2\log(1/\delta) + 2)$-bit output function χ and a sequence of random variables $X_1 \ldots X_r$ defined by $X_1 = \mathbf{E}[f(Z)]$ and

$$X_i = \mathbf{x}_i(Z_i, \chi_{i-1}(Z_{\leq i-1})) \tag{13}$$

for

- $\chi_i(z_{\leq i}) = \chi(i, z_i, \chi_{i-1}(z_{\leq i-1}))$ and letting $\chi_1(\emptyset) = \emptyset$,
- $\mathbf{x}_i(z_i, \mathsf{agt}_{i-1}) = \mathsf{rnd}_\delta\left(\mathbf{E}\left[f(Z_{\leq i}) \mid Z_i = z_i, \chi_{i-1}(Z_{\leq i-1}) = \mathsf{agt}_{i-1}\right]\right)$,
- The output of $\chi(i, z_i, \mathsf{agt}_{i-1} = (\ldots, \mathsf{aux}_{i-1}))$ is of the form $(x_i, \ldots, \mathsf{aux}_i = g(x_i, z_i, \mathsf{aux}_{i-1}))$ for $x_i = \mathbf{x}_i(z_i, \mathsf{agt}_{i-1})$,

such that

$$\Pr\left[\bigvee_{i=1}^{r-1} |X_{i+1} - X_i| \geq 1/32\sqrt{r}\right] \geq \frac{1}{5} \tag{14}$$

Namely, using the terminology of Section 4, the sequence $X_1 \ldots X_r$ is the Doob augmented weak martingales of (Z, f, χ, δ) where χ is a normal form function that augments g. As the name suggests, the sequence $X_1 \ldots X_r$ admits the (2δ-weak) martingale property (c.f. Definition 2.13). By Theorem 4.3, there exists a normal form function χ that augments g such that Equation (14) holds true, i.e., with constant probability, two consecutive points of the the sequence will be at least $1/32\sqrt{r}$ far apart. We elaborate further on this sequence.

By the correctness of the protocol, $f(Z_{\leq r}) = Y_r = \mathsf{out}$, where out denotes the output of the protocol. Thus, X_i, for $i \in [r]$, is simply the discretized expected outcome of the protocol given the two preceding values of the backup sequence $Y_i^{\mathbb{S}} = y_i$ and $Y_{i-1}^{\mathbb{S}} = y_{i-1}$, as well as a "short" string agt_{i-1} of aggregated information about the history of the execution. For our purposes, it is important to emphasize that the string agt_{i-1} is of the form $(x_{i-1}, \ldots, \mathsf{aux}_{i-1})$, where x_{i-1} is the value of the X-sequence at the previous point (i.e. the value of X_{i-1}), and aux_{i-1} is a bit indicating whether, for some $j < i-1$, either $Y_j^{\mathbb{S}}$ or $Y_{j-1}^{\mathbb{S}}$ deviated from the value of X_j by more than $1/64\sqrt{r}$. Moreover, the output of χ is of size $(\log(r) + 2\log(1/\delta) + 2)$-bit

Remark 3.12 (Computing $X_1 \dots X_r$)**.** *Each X_i is fully determined by the index i, value of Z_i and the output of $\chi_{i-1}(Z_{\leq i})$. Note that $|\chi_{i-1}(Z_{\leq i})| = (\log r + 2\log 1/\delta + 2)$, $|\mathrm{supp}(Z_i)| = \binom{n}{k} \in O(n^k)$, $|\mathrm{supp}(X_i)| = 1/\delta$, and $n^k \geq r$. Hence, there exists a table of size $\log(1/\delta) \cdot \binom{n}{k} \cdot 4 \cdot (r/\delta)^2$, such that the value of X_i, for all $i \in [r]$ can be computed from $Z_{\leq i}$ using this table. Hereafter, we fix $\delta = 1/100r$ and thus the table above table is a string of size polynomial in n^k.*

3.1.2 The Attack

We start with a high-level overview of the attack. The adversary biasing a party $h \in \mathcal{H}$, to be chosen at random, towards zero is defined as follows (the attack biassing toward one is defined analogously). After receiving the honest party messages for round $i-1$, it computes the values of $y_i = Y_i^{\mathbb{S}}$, $y_{i-1} = Y_{i-1}^{\mathbb{S}}$, $x_i = X_i$ and aux_i, for X_i and aux_i being according to Equation (13).

If y_{i-1} is below x_i by more than $1/64\sqrt{r}$, then it aborts all parties but a random tuple of $\mathbb{S}'$ that contains h, *without* sending the i^{th}-round messages of the aborting parties. The surviving corrupted parties are instructed to terminate the protocol honestly.

If y_i is below $x_i = X_i$ by more than $1/64\sqrt{r}$, it aborts all parties but a random tuple of $\mathbb{S}'$ that contains h, *after* sending the i^{th}-round messages of the aborting parties. The surviving corrupted parties are instructed to terminate the protocol honestly.

The attacker is formally defined as follows.

Algorithm 3.13 (The martingale attack $\mathsf{MartAttack}$)**.**

Parameters: $\mathbb{S}$, $\mathbb{S}' \subseteq \binom{n}{k}$, $z \in \{0,1\}$, *honest party* $h \in [n]$ *and string* $\mathsf{adv} \in \{0,1\}^*$.

Description:

1. *Compute $Y_1^{\mathbb{S}}$ according to the protocols specifications. If $(-1)^{1-z} \cdot (Y_1^{\mathbb{S}} - \frac{1}{2}) > 1/64\sqrt{r}$,* without *sending their 1st round messages, abort all parties except a random tuple in $\mathbb{S}'(h)$.*
   - *The remaining corrupted parties are instructed to terminate the protocol honestly.*
2. *For $i = 1 \dots r$:*
   (a) *Upon receiving the i^{th} round messages of h, compute $Y_i^{\mathbb{S}}$, $Y_{i+1}^{\mathbb{S}}$, X_{i+1} and aux_i using the messages received so far and the string* adv.
   (b) *If $(-1)^{1-z} \cdot (Y_i^{\mathbb{S}} - X_{i+1}) > 1/64\sqrt{r}$ and $\mathsf{aux}_i = 1$,* without *sending their messages for round i abort all parties except a random tuple in $\mathbb{S}'(h)$.*
      - *The remaining corrupted parties are instructed to terminate the protocol honestly.*
   (c) *If $(-1)^{1-z} \cdot (Y_{i+1}^{\mathbb{S}} - X_{i+1}) > 1/64\sqrt{r}$ and $\mathsf{aux}_i = 1$,* after *sending their messages for round i, abort all parties except a random tuple in $\mathbb{S}'(h)$.*
      - *The remaining corrupted parties are instructed to terminate the protocol honestly.*

Let $\mathsf{MartAttack}(\mathbb{S}, \mathbb{S}', z, h, \mathsf{adv})$ denote the martingale attacker with parameters $\mathbb{S}, \mathbb{S}', z, h, \mathsf{adv}$.

We refer to the round in which the adversary instructs some parties in its control to abort as the *aborting round*, set to r is not abort happen.

3.1.3 Success probability of Algorithm 3.13.

Let $\mathbb{S}$, $\mathbb{S}'$ and $\mathcal{H}$ be as in Lemma 3.11, and let H denote an element of $\mathcal{H}$ chosen uniformly at random. Following the discussion of Remark 3.12, let adv denote a string of size polynomial in n^k that fully describes the sequence $X_1 \dots X_r$ which is defined according to Equation (13). We show that either $\mathsf{A}_1(H) = \mathsf{MartAttack}(\mathbb{S}, \mathbb{S}', 1, H, \mathsf{adv})$ or $\mathsf{A}_0(H) = \mathsf{MartAttack}(\mathbb{S}, \mathbb{S}', 0, H, \mathsf{adv})$ succeeds in obtaining the bias of Lemma 3.11.

Before proceeding with the proof, we introduce a last piece of notation. For $z \in \{0,1\}$, let J^{z*} denote the round-index where the adversary A^z decided to abort certain parties, and let J^z denote the round-index of the last messages sent by those aborting parties. Namely, in Step 2b of Algorithm 3.13 we have $J^z = J^{z*} - 1 = i$ and in Step 2c of Algorithm 3.13 we have $J^z = J^{z*} = i+1$. If no abort occurred, $J^z = J^{z*} = r$.

Lemma 3.11 follows from the claims below.

Claim 3.14. $\Pr\left[J^1 \neq r\right] + \Pr\left[J^0 \neq r\right] \geq 1/5$

Claim 3.15. *For $z \in \{0,1\}$, $\mathbf{E}\left[X_{J^{z*}}\right] \in 1/2 \pm \frac{1}{100r}$*

Claim 3.16. $\mathbf{E}\left[\max_i |Y_i^{\mathbb{S}} - Y_i^{\mathbb{S}'}|\right] \leq 1/128\sqrt{r}$*, for r large enough.*

Before proving each of these claims, we show how to combine them to obtain the lemma.

Proof of Lemma 3.11. By Claim 3.14, we may assume without loss of generality that $\Pr\left[J^1 \neq r\right] \geq 1/10$. Next, we compute the bias caused by the attacker $\mathsf{A}_1(H)$. Notice that the output of the honest party is identically distributed with $Y_{J^1}^{\mathbb{S}'}$. Compute

$$\begin{aligned}
\mathbf{E}\left[Y_{J^1}^{\mathbb{S}'}\right] - 1/2 &\geq \mathbf{E}\left[Y_{J^1}^{\mathbb{S}}\right] - 1/2 - \mathbf{E}\left[Y_{J^1}^{\mathbb{S}}\right] + \mathbf{E}\left[Y_{J^1}^{\mathbb{S}'}\right] \\
&\geq \mathbf{E}\left[Y_{J^1}^{\mathbb{S}}\right] - \mathbf{E}\left[X_{J^{1*}}\right] - \mathbf{E}\left[\max_i \left|Y_i^{\mathbb{S}} - Y_i^{\mathbb{S}'}\right|\right] \cdot \Pr\left[J^1 \neq r\right] - \frac{1}{100r} \qquad (15) \\
&\geq \Pr\left[J^1 \neq r\right] \cdot \left(\mathbf{E}\left[Y_{J^1}^{\mathbb{S}} - X_{J^{1*}} \mid J^1 \neq r\right] - \mathbf{E}\left[\max_i \left|Y_i^{\mathbb{S}} - Y_i^{\mathbb{S}'}\right|\right]\right) - \frac{1}{100r} \qquad (16) \\
&\geq \Pr\left[J^1 \neq r\right] \left(\frac{1}{64\sqrt{r}} - \frac{1}{128\sqrt{r}}\right) - \frac{1}{100r} \\
&\geq \frac{1}{10} \cdot \frac{1}{128\sqrt{r}} - \frac{1}{100r}.
\end{aligned}$$

Equation (15) follows from triangle inequality and union bound and Claim 3.15, and Equation (16) follows from Claim 3.16 and the fact that $Y_{J^1}^{\mathbb{S}} - X_{J^{1*}} \geq 1/64\sqrt{r}$, whenever $J^1 \neq r$. □

Proof of Claim 3.14. First, we lower-bound the probability of abort by the probability of having a large increment in the X-sequence alone. For convenience, we introduce the following notation. For $z \in \{0,1\}$, let trig_{i+1}^z denote the predicate $(-1)^{1-z}(Y_i^{\mathbb{S}} - X_{i+1}) \geq 1/64\sqrt{r} \ \vee \ (-1)^{1-z}(Y_{i+1}^{\mathbb{S}} - X_{i+1}) \geq 1/64\sqrt{r}$ and let trig_1^z denote the predicate $(-1)^{1-z}(Y_1^{\mathbb{S}} - \frac{1}{2}) \geq 1/64$. Write $\mathsf{trig}_{i+1} = \mathsf{trig}_{i+1}^0 \vee \mathsf{trig}_{i+1}^1$. Recall that

$$\Pr\left[J^z \neq r\right] = \Pr\left[\mathsf{trig}_1^z \vee \bigvee_{i=1}^{r-1} \left(\mathsf{aux}_i = 1 \wedge \mathsf{trig}_{i+1}^z\right)\right].$$

Thus, by union bound,

$$\Pr\left[J^0 \neq r\right] + \Pr\left[J^1 \neq r\right] \geq \Pr\left[\mathsf{trig}_1 \vee \bigvee_{i=1}^{r-1} \left(\mathsf{aux}_i = 1 \wedge \mathsf{trig}_{i+1}\right)\right].$$

Recall that $\mathsf{aux}_i = 1$ is equivalent to $\bigwedge_{j=1}^{i} \neg\mathsf{trig}_j \equiv \neg\left(\bigvee_{j=1}^{i} \mathsf{trig}_j\right)$. It follows that

$$\begin{aligned}\bigvee_{i=1}^{r-1} \left(\mathsf{aux}_i = 1 \wedge \mathsf{trig}_{i+1}\right) &\equiv \bigvee_{i=1}^{r-1} \left(\mathsf{trig}_{i+1} \wedge \neg\left(\bigvee_{j=1}^{i} \mathsf{trig}_j\right)\right) \\ &\equiv \bigvee_{i=1}^{r-1} \mathsf{trig}_{i+1}.\end{aligned}$$

We can thus lower-bound $\Pr\left[J^0 \neq r\right] + \Pr\left[J^1 \neq r\right]$ by $\Pr\left[\bigvee_{i=1}^{r-1} \mathsf{trig}_{i+1}\right]$.

$$\begin{aligned}\Pr\left[J^0 \neq r\right] + \Pr\left[J^1 \neq r\right] &\geq \Pr\left[\mathsf{trig}_1 \vee \bigvee_{i=1}^{r-1} \mathsf{trig}_{i+1}\right] \\ &= \Pr\left[\left|Y_1^{\mathbb{S}} - X_1\right| \vee \bigvee_{i=1}^{r-1} \left(\left|Y_i^{\mathbb{S}} - X_{i+1}\right| \geq 1/64\sqrt{r} \vee \left|Y_{i+1}^{\mathbb{S}} - X_{i+1}\right| \geq 1/64\sqrt{r}\right)\right] \\ &= \Pr\left[\bigvee_{i=1}^{r-1} \left(\left|Y_i^{\mathbb{S}} - X_i\right| \geq 1/64\sqrt{r} \vee \left|Y_i^{\mathbb{S}} - X_{i+1}\right| \geq 1/64\sqrt{r}\right)\right] \\ &\geq \Pr\left[\bigvee_{i=1}^{r-1} |X_{i+1} - X_i| \geq 1/32\sqrt{r}\right]\end{aligned}$$

By Equation (14), we conclude that $\Pr\left[\bigvee_{i=1}^{r-1} |X_{i+1} - X_i| \geq 1/32\sqrt{r}\right] \geq 1/5$.

□

Proof of Claim 3.15. Recall that $\mathbf{E}\left[X_i\right] = \mathbf{E}\left[\mathsf{rnd}_\delta(\mathbf{E}\left[\mathsf{out} \mid Z_i, \chi_{i-1}(Z_{\leq i-1})\right])\right]$ and that we fixed $\delta = 1/100r$. We compute $\mathbf{E}\left[X_{J^{z*}}\right] = \sum_i \mathbf{E}\left[X_i \mid J^{z*} = i\right] \cdot \Pr\left[J^{z*} = i\right]$. Let us focus on the term $\mathbf{E}\left[X_i \mid J^{z*} = i\right]$.

$$\begin{aligned}\mathbf{E}\left[X_i \mid J^{z*} = i\right] &= \mathbf{E}\left[\mathsf{rnd}_\delta(\mathbf{E}\left[\mathsf{out} \mid Z_i, \chi_{i-1}(Z_{\leq i-1})\right]) \mid J^{z*} = i\right] \\ &\in \mathbf{E}\left[\mathbf{E}\left[\mathsf{out} \mid Z_i, \chi_{i-1}(Z_{\leq i-1})\right] \mid J^{z*} = i\right] \pm \delta.\end{aligned} \tag{17}$$

Recall that $Z_i, \chi_{i-1}(Z_{\leq i-1})$ fully determine X_i, Y_i, Y_{i-1} and $J^{z*} \geq i$. Thus $Z_i, \chi_{i-1}(Z_{\leq i-1})$ fully determine $J^{z*} = i$, which implies that

$$\mathbf{E}\left[\mathbf{E}\left[\mathsf{out} \mid Z_i, \chi_{i-1}(Z_{\leq i-1})\right] \mid J^{z*} = i\right] = \mathbf{E}\left[\mathsf{out} \mid J^{z*} = i\right] \tag{18}$$

Since, by assumption, $\mathbf{E}\left[\mathsf{out}\right] = 1/2$, it follows that $\mathbf{E}\left[X_{J^{z*}}\right] \in \mathbf{E}\left[\mathsf{out}\right] \pm \delta = 1/2 \pm \frac{1}{100r}$. □

Proof of Claim 3.16. From the hypothesis of the theorem, it holds that

$$\forall \rho \in \{1, 1+1/r, \ldots, r\}, \quad \Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}} - Y_i^{\mathbb{S}'}\right| \geq \rho \cdot \frac{1}{256\sqrt{r}}\right] \leq \frac{1}{2\rho \log(r)} \ .$$

For convenience, write $Y_{\max} = \max_{i\in[r]} \left|Y_i^{\mathbb{S}} - Y_i^{\mathbb{S}'}\right|$ and let us compute $\mathbf{E}[Y_{\max}]$.

$$\begin{aligned}
\mathbf{E}[Y_{\max}] &= \mathbf{E}\left[Y_{\max} \mid Y_{\max} \leq 1/256\sqrt{r}\right] \cdot \Pr\left[Y_{\max} \leq 1/256\sqrt{r}\right] \\
&\quad + \sum_{j=1}^{\log(256\sqrt{r})} \mathbf{E}\left[Y_{\max} \mid 256\sqrt{r} \cdot Y_{\max} \in [2^{j-1}, 2^j]\right] \cdot \Pr\left[256\sqrt{r} \cdot Y_{\max} \in [2^{j-1}, 2^j]\right] \\
&\leq \frac{1}{256\sqrt{r}} + \sum_{j=1}^{\log(256\sqrt{r})} \frac{2^j}{256\sqrt{r}} \cdot \frac{1}{2^{j-1} \cdot 2\log(r)} \\
&= \frac{1}{256\sqrt{r}} + \frac{1}{256\sqrt{r}\log(r)} \cdot \left(\frac{1}{2} \cdot \log(r) + \log(256)\right) \\
&\leq \frac{1}{128\sqrt{r}} \ ,
\end{aligned}$$

where the last inequality holds for large enough r. □

3.2 The Differential Privacy Based Attack

Lemma 3.17 (Restatement of Lemma 3.9)**.** *There exists a fails-stop adversary* A *such that the following holds. Let* Π *be a correct* n*-party* r*-round coin-flipping protocol, and let* $k \in \mathbb{N}$ *be the smallest integer such that* $\binom{n}{k} \geq r\log(r)^{2k}$*. Suppose there exists* $k^* \in \{2, \ldots, k\}$*,* $\rho^* \in \{1, 1+1/r, \ldots, r\}$*, tuple sets* $\mathbb{S}_1$ *and* $\mathbb{S}_0 \subseteq \binom{[n]}{k}$ *and party set* $\mathcal{H} \subseteq [n]$*, such that*

- *For every* $h, h' \in \mathcal{H}$*,* $z, z' \in \{0,1\}$ *and* $\mathcal{U}' \in \mathbb{S}_z$*:*
  - $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h' \in \mathcal{U}] \leq \frac{1}{2}$.
  - $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_{z'}}[h \in \mathcal{U}]$.
  - $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \notin \mathcal{U}] / \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] \geq \frac{1}{4} \cdot \frac{n-k+k^*-1}{k^*-1}$.
  - $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}_z(h)}[\mathcal{U} = \mathcal{U}'] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[\mathcal{U} = \mathcal{U}']$.
- *Letting* $Y_i^{\mathbb{S}_z} = Y_i^{\mathbb{S}_z}(\Pi)$ *and* $\mathsf{coef}_n(k,\cdot)$ *be according is according to Definition 3.4 and Notation 3.3:*

$$\Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0}\right| \geq \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*)^{1/2}}{(64\log(r))^{k-k^*}}\right] \geq \frac{1}{2\rho^*\log(r)} \cdot \frac{64^{-k+k^*}}{\mathsf{coef}_n(k,k^*)^{1/2}} \tag{19}$$

- *Letting* $Y_i^{\mathbb{S}_z(h)} = Y_i^{\mathbb{S}_z(h)}(\Pi)$ *be according to Definition 3.4, for every* $z \in \{0,1\}$*,* $h, h' \in \mathcal{H}$ *and* $\rho \in \{1, 1+1/r, \ldots, r\}$*, it holds that:*

$$\Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}_z(h)} - Y_i^{\mathbb{S}_z(h')}\right| \geq \frac{\rho}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*-1)^{1/2}}{(64\log(r))^{k-k^*+1}}\right] \leq \frac{1}{2\rho\log(r)} \cdot \frac{64^{-k+k^*-1}}{\mathsf{coef}_n(k,k^*-1)^{1/2}} \tag{20}$$

Then, there exists $h \in \mathcal{H}$ such that $\mathsf{A}^{\Pi}(\mathbb{S}_1, \mathbb{S}_0, \mathcal{H}, k^*, \rho^*)$ corrupting all parties but h biases the output of h by $O(1/\sqrt{r}\log(r)^{k-k^*+1})$.

Furthermore, the running time of $\mathsf{A}^{\Pi}(\mathbb{S}_1, \mathbb{S}_0, \mathcal{H}, k^*, \rho^*)$ is polynomial in the running time of Π and n^k, and it uses only oracle access to Π's next-message function.

3.2.1 The Attack

We start with an high-level overview of the attack using the notation of Lemma 3.17.

The adversary corrupts all parties except a random party $h \in \mathcal{H}$. After receiving the honest party i^{th} message, it adds Laplace noise to the quantity $Y_i^{\mathbb{S}_1 \setminus h} - Y_i^{\mathbb{S}_0 \setminus h}$, i.e., the difference between the average backup values for those tuples that do not contain h. If the resulting quantity is above some value γ, the adversary aborts all parties except a random tuple in $\mathbb{S}_z(h)$, for $z \in \{0,1\}$ being the direction of the bias the adversary wishes to attack towards[6].

Since, by assumption, the values $Y_i^{\mathbb{S}_z \setminus h}$ and $Y_i^{\mathbb{S}_z(h)}$ are not too far apart, adding Laplace noise "decorrelates" the abort decision from the identity of the honest party party h. Thus, $Y_i^{\mathbb{S}_z(h)}$ is roughly distributed like the mean $Y_i^{\mathbb{S}_z}$ (and by extension $Y_i^{\mathbb{S}_z \setminus h}$ as well). Therefore, either the adversary biasing towards one or the adversary biasing towards zero succeeds in its attack, since either $\mathbf{E}\left[Y_J^{\mathbb{S}_1}\right] > 1/2$ or $\mathbf{E}\left[Y_J^{\mathbb{S}_0}\right] < 1/2$, where J denote the aborting round.

The formal description of the attack is given below.

Algorithm 3.18 (DpAttack: The Differential Privacy Based Attack)**.**

Parameters: $\mathbb{S}_1, \mathbb{S}_0 \subseteq \binom{n}{k}$, $z \in \{0,1\}$, *party* $h \in [n]$ *and* $\gamma \in [0,1]$.

Notation: Let $\lambda = \gamma/4\log(r)$.

Description:

1. *For* $i = 1 \ldots r$*:*
   (a) *Upon receiving the i^{th}-round messages of h, compute $Y_i^{\mathbb{S}_1 \setminus h}$ and $Y_i^{\mathbb{S}_0 \setminus h}$.*
   (b) *Sample* $\nu_i \leftarrow \mathsf{Lap}(\lambda)$.
   (c) *If* $Y_i^{\mathbb{S}_1 \setminus h} - Y_i^{\mathbb{S}_0 \setminus h} + \nu_i > \gamma$*, without sending their messages for round i, abort all parties except a random tuple in* $\mathbb{S}_z(h)$.
      – *The remaining corrupted parties are instructed to terminate the protocol honestly.*

Let $\mathsf{DpAttack}(\mathbb{S}_1, \mathbb{S}_0, z, h, \gamma)$ denote the above attacker with parameters $\mathbb{S}_1, \mathbb{S}_0, z, h, \gamma$. We refer to the round in which the adversary instructs some parties in its control to abort as the *aborting round*, set to r is not abort happen.

3.2.2 Success probability of Algorithm 3.18

Let H be a uniform element of $\mathcal{H}$, and let $\gamma = \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*)^{1/2}}{(64\log(r))^{k-k^*}}$. We show that either $\mathsf{A}_1(H) = \mathsf{DpAttack}(\mathbb{S}_1, \mathbb{S}_0, 1, H, \gamma)$ or $\mathsf{A}_0(H) = \mathsf{DpAttack}(\mathbb{S}_1, \mathbb{S}_0, 0, H, \gamma)$ succeeds in obtaining the bias of

[6]The choice of γ and of Laplace parameter is dictated by the magnitude of the gap between $Y_i^{\mathbb{S}_1}$ and $Y_i^{\mathbb{S}_0}$ as stated in Equation (19).

Lemma 3.17. Let J denote the smallest round i such that $Y_i^{\mathbb{S}_1 \setminus H} - Y_i^{\mathbb{S}_0 \setminus H} + \mathsf{Lap}(\lambda) \geq \gamma$, and $J = r$ if no such round exists. Lemma 3.17 follows from the next claim.

Claim 3.19. $\mathbf{E}\left[Y_J^{\mathbb{S}_1(H)} - Y_J^{\mathbb{S}_0(H)}\right] \geq \frac{1}{2^{16}} \cdot \frac{1}{\sqrt{r}\log r} \cdot \left(\frac{1}{64^2 \log(r)}\right)^{k-k^*}$.

Proof of Lemma 3.17. If $\mathbf{E}\left[Y_J^{\mathbb{S}_1(H)} - Y_J^{\mathbb{S}_0(H)}\right] \geq \varepsilon$, then either $\mathbf{E}\left[Y_J^{\mathbb{S}_1(H)}\right] \geq 1/2 + \varepsilon/2$ or $\mathbf{E}\left[Y_J^{\mathbb{S}_0(H)}\right] \leq 1/2 - \varepsilon/2$. By using the appropriate ε from Claim 3.19 and observing that, under adversary A_z, the honest party's output is identically distributed with $Y_J^{\mathbb{S}_z(H)}$, we obtain the desired statement. □

Proof of Claim 3.19. Define $\delta = \frac{1}{2} \cdot \frac{1}{2\rho^* \log(r)} \cdot \frac{64^{-k+k^*}}{\mathsf{coef}_n(k,k^*)^{1/2}}$, $\alpha = \frac{\gamma}{32\log(r)} \cdot \frac{\sqrt{n-k+k^*-1}}{\sqrt{k^*-1}}$ and $\beta = \frac{\delta}{16} \cdot \frac{\sqrt{k^*-1}}{\sqrt{n-k+k^*-1}}$. From the hypothesis of Lemma 3.17 and the choice of α, β, γ and δ, the following inequalities hold without loss of generality.

$$\Pr\left[\max_i Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0} \geq \gamma\right] \geq \delta \tag{21}$$

$$\forall h \in \mathcal{H}\colon \qquad \Pr\left[\max_i \left|Y_i^{\mathbb{S}_1(h)} - Y_i^{\mathbb{S}_0(h)} - Y_i^{\mathbb{S}_1} + Y_i^{\mathbb{S}_0}\right| \geq \rho \cdot \alpha\right] \leq \beta/\rho \tag{22}$$

Let τ denote an arbitrary transcript of Π and let $s_i^h(\tau)$ and $s_i^{\setminus h}(\tau)$ denote the value of $Y_i^{\mathbb{S}_1(h)} - Y_i^{\mathbb{S}_0(h)}$ and $Y_i^{\mathbb{S}_1 \setminus h} - Y_i^{\mathbb{S}_0 \setminus h}$, respectively, for transcript τ. Further define $s_i(\tau) = \sum_{h \in \mathcal{H}} s_i^h(\tau)$, and, for arbitrary $h \in \mathcal{H}$ and $z \in \{0,1\}$, let $p = \Pr_{u \leftarrow \mathbb{S}_z}[h \in u]$. We remark that the value of p does not depend on h or z. Next, by the definition of $s_i^h(\tau)$ and the hypothesis of the theorem, we observe that

1. $p \cdot s_i^h(\tau) + (1-p) \cdot s_i^{\setminus h}(\tau) = s_i(\tau)$, and
2. $\frac{1-p}{p} \geq \frac{1}{4} \cdot \frac{n-k+k^*-1}{k^*-1}$

By definition, the adversary A_z aborts (some parties) if it find out that $s_i^{\setminus h}(\tau) + \mathsf{Lap}(\lambda) \geq \gamma$. Let T be the value of τ, and J be the aborting round in a random execution of Π in which the adversary A_z attacking the honest party H. Using the terminology of Section 5, the value of $s_J^H(T)$ is equal to the output of an oblivious sampling experiment with parameters $\mathcal{H}$, $\left\{s_i^h(\tau \leftarrow T)\right\}_{h,i}$, γ, p, λ. From the choice of α and β, and under the guarantee of Equation (22), Corollary 5.3 yields that $\mathbf{E}\left[s_J^H(T)\right] \geq \gamma\delta/64$, for r large enough.

□

3.3 The Singletons Attack

Lemma 3.20 (Restatement of Lemma 3.10)**.** *There exists a fails-stop adversary* A *such that the following holds. Let* Π *be a correct* n*-party* r*-round coin-flipping protocol, and let* $k \in \mathbb{N}$ *be the smallest integer such that* $\binom{n}{k} \geq r\log(r)^{2k}$*. Suppose there exists* $\rho^* \geq 1$*, tuple sets* $\mathbb{S}_1, \mathbb{S}_0 \subseteq \binom{[n]}{k}$ *and party set* $\mathcal{H} \subseteq [n]$ *such that:*

1. $\mathcal{H} \geq n/3$ *and* $|\mathbb{S}_0| = |\mathbb{S}_1| = |\mathcal{H}|$.

For every $h \in \mathcal{H}$ and $z \in \{0,1\}$:

2. $|\mathbb{S}_z(h)| = 1$, *letting $\mathbb{S}_z(h)$ be according to Notation 3.3.*

3. $\Pr\left[\max_{i\in[r]}\left|Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0}\right| \geq \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\binom{n-1}{k-1}^{1/2}}{(64\log(r))^{k-1}}\right] \geq \frac{1}{2\rho^*\log(r)} \cdot \frac{64^{-k+1}}{\binom{n-1}{k-1}^{1/2}}$

   letting $Y_i^{\mathbb{S}_z}$ be according to Definition 3.4.

Then, there exists $h \in \mathcal{H}$ such that $\mathsf{A}^{\Pi}(\mathbb{S}_1, \mathbb{S}_0, \mathcal{H}, k^*, \rho^*)$ corrupting all parties but h, biases the output of h by $O(1/\sqrt{r}\log(r)^k)$.

Furthermore, the running time of $\mathsf{A}^{\Pi}(\mathbb{S}_1, \mathbb{S}_0, \mathcal{H}, k^*, \rho^*)$ is polynomial in the running time of Π and n^k, and it uses only oracle access to Π's next-message function.

3.3.1 The Attack

We start with a high-level overview of the attack. The adversary biasing a party $h \in \mathcal{H}$, to be chosen at random, towards zero is defined as follows (the attack biassing toward one is defined analogously). Before the protocols starts, the adversary samples *half* of the tuples in $\mathbb{S}_1$ and $\mathbb{S}_0$ not containing h, denoted $\mathbb{E}_1$ and $\mathbb{E}_0$ respectively. Upon receiving the i^{th} message from h, it computes the difference between the average backup values of the tuples in $\mathbb{E}_1$ and $\mathbb{E}_0$, denoted $Y_i^{\mathbb{E}_1} - Y_i^{\mathbb{E}_0}$. If the resulting quantity is above $3\gamma/4$, it aborts all parties except the unique tuple in $\mathbb{S}_0(h)$.[7] For the attack to go through, it is required that $Y_i^{\mathbb{E}_z}$ and $Y_i^{\mathbb{S}_z}$ are not too far apart. Thankfully, standard concentration bounds guarantee that to be the case.

The formal description of the attack is given below.

Algorithm 3.21 (The Singletons attacker $\mathsf{SingAttack}$)**.**

Parameters: tuple subsets $\mathbb{S}_1, \mathbb{S}_0 \subseteq \binom{n}{k}$, $z \in \{0,1\}$, honest party $h \in [n]$ and $\gamma \in [0,1]$.

Description:

1. *For $z \in \{0,1\}$, let $\mathbb{E}_z \subseteq \mathbb{S}_z \setminus h$ denote random subset of size $|\mathbb{S}_z|/2$.*
2. *For $i = 1 \ldots r$:*
   (a) *Upon receiving the i^{th}-round messages of h, compute $Y_i^{\mathbb{E}_1}$ and $Y_i^{\mathbb{E}_0}$.*
   (b) *If $Y_i^{\mathbb{E}_1} - Y_i^{\mathbb{E}_0} > 3\gamma/4$, without sending their messages for round i, abort all parties except a random tuple in $\mathbb{S}_z(h)$.*
      – *The remaining corrupted parties are instructed to terminate the protocol honestly.*

Let $\mathsf{SingAttack}(\mathbb{S}_1, \mathbb{S}_0, z, h, \gamma)$ denote the singletons attacker with parameters $\mathbb{S}_1, \mathbb{S}_0, z, h$. We refer to the round in which the adversary instructs some parties in its control to abort as the *aborting round*, set to r is not abort happen.

[7] The choice of γ is dictated by the magnitude of the gap between $Y_i^{\mathbb{S}_1}$ and $Y_i^{\mathbb{S}_0}$ as stated in Assumption (3).

3.3.2 Success probability of Algorithm 3.21

Let H be a uniform element of $\mathcal{H}$. Let $\gamma = \alpha/\sqrt{n}$ letting $\alpha = \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\sqrt{k}\cdot\binom{n}{k}^{1/2}}{(64\log(r))^{k-1}}$. We show that either $\mathsf{A}_1(H) = \mathsf{SingAttack}(\mathbb{S}_1, \mathbb{S}_0, 1, H, \gamma)$ or $\mathsf{A}_0(H) = \mathsf{SingAttack}(\mathbb{S}_1, \mathbb{S}_0, 0, H, \gamma)$ succeeds in obtaining the bias of Lemma 3.20. Let J denote the smallest round i such that $Y_i^{\mathbb{E}_1} - Y_i^{\mathbb{E}_0} \geq 3\gamma/4$, and $J = r$ if no such round exists. Furthermore, define $\beta = \frac{1}{2\rho^*\log(r)} \cdot \frac{64^{k-1}}{\binom{n-1}{k-1}^{1/2}}$, let $G_{r,\alpha}$ denote the event $\max_i \left\{ Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0} \right\} \geq \alpha/\sqrt{n}$, let $E_{r,\alpha}$ denote the event $(\max_i \left\{ \left| Y_i^{\mathbb{E}_1} - Y_i^{\mathbb{S}_1} \right| \right\} \geq \alpha/8\sqrt{n}) \vee (\max_i \left\{ \left| Y_i^{\mathbb{E}_0} - Y_i^{\mathbb{S}_0} \right| \right\} \geq \alpha/8\sqrt{n})$. Lemma 3.20 follows from Claims 3.22 and 3.23.

Claim 3.22. $\Pr\left[J \neq r \mid G_{r,\alpha} \wedge \neg E_{r,\alpha}\right] = 1$.

Claim 3.23. $\Pr\left[E_{r,\alpha}\right] \leq 4r \cdot \exp(-\alpha^2/192) \leq \frac{1}{r}$, *for r large enough.*

We prove Lemma 3.20 assuming the two claims above.

Proof of Lemma 3.20. First we observe that, under adversary $\mathsf{A}_z(H)$, the honest party's output is identically distributed with $Y_J^{\mathbb{S}_z(H)}$. Thus, like in the proof of Lemma 3.17, it suffices to lower-bound $\mathbf{E}\left[Y_J^{\mathbb{S}_1(H)} - Y_J^{\mathbb{S}_0(H)}\right]$. By the choice of α and β, $\Pr\left[G_{r,\alpha}\right] \geq \beta$. Consequently,

$$\begin{aligned}
\mathbf{E}\left[Y_J^{\mathbb{S}_1(H)} - Y_J^{\mathbb{S}_0(H)}\right] &\geq \mathbf{E}\left[Y_J^{\mathbb{S}_1(H)} - Y_J^{\mathbb{S}_0(H)} \mid G_{r,\alpha} \wedge \neg E_{r,\alpha}\right] \cdot \Pr\left[G_{r,\alpha} \wedge \neg E_{r,\alpha}\right] - \Pr\left[E_{r,\alpha}\right] \\
&\geq \left(\mathbf{E}\left[Y_J^{\mathbb{E}_1} - Y_J^{\mathbb{E}_0} \mid G_{r,\alpha} \wedge \neg E_{r,\alpha}\right] - \frac{\alpha}{4\sqrt{n}}\right) \cdot \Pr\left[G_{r,\alpha} \wedge \neg E_{r,\alpha}\right] - \Pr\left[E_{r,\alpha}\right] \\
&\geq \frac{1}{2} \cdot \frac{\alpha}{\sqrt{n}} \cdot \Pr\left[G_{r,\alpha}\right] - 2 \cdot \Pr\left[E_{r,\alpha}\right] \geq \frac{\alpha\beta}{2\sqrt{n}} - 2 \cdot \Pr\left[E_{r,\alpha}\right] \\
&\geq \frac{1}{1024\sqrt{r}\log(r)} \cdot \left(\frac{1}{64^2 \cdot \log(r)}\right)^{k-1} - \frac{2}{r} \ .
\end{aligned}$$

□

Proof of Claim 3.22. If $E_{r,\alpha}$ did not occur, then $Y_i^{\mathbb{E}_1} - Y_i^{\mathbb{E}_0}$ differs from $Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0}$ by at most $\frac{\alpha}{4\sqrt{n}}$. If the latter is greater than $\alpha/\sqrt{n}$, then the former is greater than $\frac{3\alpha}{4\sqrt{n}} = 3\gamma/4$.

Proof of Claim 3.23. By assumption, $\binom{n}{k} \geq r\log(r)^{2k}$. It follows that

$$\alpha = \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\sqrt{k} \cdot \binom{n}{k}^{1/2}}{(64\log(r))^{k-1}} \geq \frac{\rho^*\sqrt{k} \cdot \log(r)}{2^{6k+8}} \ .$$

Thus, by noting that $|\mathcal{H}| \geq n/3$, apply union bound and Hoeffding's inequality (Fact 2.8), and deduce that

$$\Pr\left[E_{r,\alpha}\right] \leq 4r \cdot \exp(-\alpha^2/192) \leq 4r \cdot \exp(-2\log(2r)) \ ,$$

where the last inequality holds for r large enough.

3.4 Proof of Lemma 3.7

Notation 3.24. *The concatenation of two tuple subsets $\mathbb{S}_1, \mathbb{S}_0 \subseteq 2^{[n]}$, denoted $\mathbb{S}_1 \| \mathbb{S}_0$, is defined by $\{\mathcal{U}_1 \cup \mathcal{U}_0 : \mathcal{U}_1 \in \mathbb{S}_1, \mathcal{U}_0 \in \mathbb{S}_0\}$.*

For reference, we recall of the nugget Definition 3.6.

Definition 3.25 (Restatement of Definition 3.6.)**.** *Let Π be an n-party r-round coin-flipping protocol, and let $k \in \mathbb{N}$ be the smallest integer such that $\binom{n}{k} \geq r \log(r)^{2k}$. Index $k^* \in [k+1]$ is a* nugget *for Π, if there exists $\rho^* \in \mathcal{R}(r)$, set $\mathcal{H} \subseteq [n]$ and tuple sets $\mathbb{S}_1, \mathbb{S}_0 \subseteq \binom{n}{k}$ such that the following holds.*

For a tuple-set $\mathbb{S} \subseteq 2^{[n]}$ and $i \in [r]$, let $Y_i^{\mathbb{S}}$ denote the value of $\mathsf{AvgBckp}(\mathbb{S}, i)$ in a random execution of Π. The following holds according to the value of k^*:

$k^* = 1$:

1. $\Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}_1} - Y_i^{\mathbb{S}_0}\right| \geq \frac{\rho^*}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*)^{1/2}}{(64\log(r))^{k-k^*}}\right] \geq \frac{1}{2\rho^*\log(r)} \cdot \frac{64^{-k+k^*}}{\mathsf{coef}_n(k,k^*)^{1/2}}$.
2. $\mathcal{H} \geq n/3$, $|\mathbb{S}_1| = |\mathbb{S}_0| = |\mathcal{H}|$, *and* $|\mathbb{S}_z(h)| = 1$ *for every* $h \in \mathcal{H}$ *and* $z \in \{0,1\}$.

$k^* \in \{2, \ldots, k\}$:

1. *Same as Item 1 for $k^* = 1$.*
2. *For every $h, h' \in \mathcal{H}$, $z, z' \in \{0,1\}$, $\mathcal{U}' \in \mathbb{S}_z$ and $\rho \in \mathcal{R}(r)$:*
   (a) $\Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}_z(h)} - Y_i^{\mathbb{S}_z(h')}\right| \geq \frac{\rho}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,k^*-1)^{1/2}}{(64\log(r))^{k-k^*+1}}\right] \leq \frac{1}{2\rho\log(r)} \cdot \frac{64^{-k+k^*-1}}{\mathsf{coef}_n(k,k^*-1)^{1/2}}$.
   (b) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h' \in \mathcal{U}] \leq \frac{1}{2}$.
   (c) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_{z'}}[h \in \mathcal{U}]$.
   (d) $\Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \notin \mathcal{U}] / \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[h \in \mathcal{U}] \geq \frac{1}{4} \cdot \frac{n-k+k^*-1}{k^*-1}$.
   (e) $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}_z(h)}[\mathcal{U} = \mathcal{U}'] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_z}[\mathcal{U} = \mathcal{U}']$

$k^* = k + 1$:

1. $\mathbb{S}_1(h) = \emptyset$ *for every* $h \in \mathcal{H}$.
2. $\Pr_{h\leftarrow\mathcal{H},\mathcal{U}\leftarrow\mathbb{S}_0(h)}[\mathcal{U} = \mathcal{U}'] = \Pr_{\mathcal{U}\leftarrow\mathbb{S}_0}[\mathcal{U} = \mathcal{U}']$ *for every* $\mathcal{U}' \in \mathbb{S}_0$.
3. $\Pr\left[\max_{i\in[r]} \left|Y_i^{\mathbb{S}_0} - Y_i^{\mathbb{S}_1}\right| \geq \frac{\rho}{256\sqrt{r}}\right] \leq \frac{1}{2\rho\log(r)}$ *for every* $\rho \in \mathcal{R}(r)$.

Next we prove that any protocol admits a nugget.

Proof. (of Lemma 3.7)

We prove the lemma by explicitly constructing the sets (see Figure 1). From the construction of the sets, there exists $\mathcal{Q} \subseteq \mathcal{P}$ of size $(k - k^* - 1)$, parties $p_1, p_0 \in (\mathcal{P} \setminus \mathcal{Q})$ and tuple set $\mathcal{C} \in \{\mathcal{A}_1, \mathcal{A}_0\}$, such that $\mathbb{S}_z$ and $\mathcal{H}$ are of the form

$$\mathbb{S}_z = \begin{cases} \binom{\mathcal{P}}{k-1} \| \binom{\mathcal{A}_z}{1} & \text{if } k^* \in \{k, k+1\} \\ \mathcal{Q} \| \{p_z\} \| \binom{\mathcal{P}\setminus(\mathcal{Q}\cup\{p_z\})}{k^*-1} \| \binom{\mathcal{C}}{1} & \text{if } k^* \in \{1 \ldots k-1\} \end{cases}$$

$$\mathcal{H} = \begin{cases} \mathcal{A}_0 & \text{if } k^* \in \{k+1\} \\ \mathcal{P} \setminus (\mathcal{Q} \cup \{p_1, p_0\}) & \text{if } k^* \in \{2 \ldots k\} \\ \mathcal{C} & \text{if } k^* = 1 \end{cases}$$

It is easy to verify that the lemma holds for $k^* = 1$ and $k^* = k+1$ hold, so it remains to prove that it holds for $k^* \in \{2, \ldots, k\}$. We remind the reader that $k^* \leq k < \sqrt{n}$. Clearly, $\Pr_{\mathcal{U} \leftarrow \mathbb{S}^z}[h \in \mathcal{U}] = \frac{k^*-1}{|\mathcal{H}|}$ or $\frac{k^*-1}{|\mathcal{H}|+1} \leq \frac{1}{2}$, and $\Pr_{\mathcal{U} \leftarrow \mathbb{S}_z}[h \in \mathcal{U}] = \Pr_{\mathcal{U} \leftarrow \mathbb{S}_{z'}}[h \in \mathcal{U}]$. Furthermore,

$$\begin{aligned}
\frac{\Pr_{u \leftarrow \mathbb{S}^z}[h \notin u]}{\Pr_{u \leftarrow \mathbb{S}^z}[h \in u]} &\geq \frac{1 - (k^*-1)/|\mathcal{H}|}{(k^*-1)/|\mathcal{H}|} = \frac{|\mathcal{H}|}{k^*-1} - 1 \\
&\geq \frac{n/3 - (k - k^* - 1) - 2}{k^* - 1} - 1 = \frac{n/3 - k + k^* - 1}{k^* - 1} - 1 \\
&\geq \frac{1}{4} \cdot \frac{n - k + k^* - 1}{k^* - 1} \ ,
\end{aligned}$$

where the last follows from $n/3 \geq 4k + 1$, for n large enough since $\sqrt{n} > k$. Finally, $\Pr_{h \leftarrow \mathcal{H}, \mathcal{U} \leftarrow \mathbb{S}_z(h)}[\mathcal{U} = \mathcal{U}'] = \Pr_{\mathcal{U} \leftarrow \mathbb{S}_z}[\mathcal{U} = \mathcal{U}']$ follows immediately from the definition $\mathbb{S}_z$ and $\mathcal{H}$. $\square$

Let $\mathcal{A}_1, \mathcal{A}_0, \mathcal{P} \subset [n]$ denote an arbitrary equal-size partition of $[n]$ (i.e., $|\mathcal{A}_1| = |\mathcal{A}_0| = |\mathcal{P}|$ and $\mathcal{A}_1 \sqcup \mathcal{A}_0 \sqcup \mathcal{P} = [n]$, without loss of generality n is a multiple of 3).

Define $k^* \in [k+1]$, $\mathbb{S}_1 \subseteq, \mathbb{S}_0 \subseteq \binom{[n]}{k}, \mathcal{H} \subseteq [n]$ and $\rho^* \in \mathcal{R}(r)$ by the following iterative process:

1. Let $\mathbb{S}_1^{k+1} = \binom{\mathcal{A}_1}{1} \| \binom{\mathcal{P}}{k-1}$, $\mathbb{S}_0^{k+1} = \binom{\mathcal{A}_0}{1} \| \binom{\mathcal{P}}{k-1}$, $\mathcal{H}_{k+1} = \mathcal{A}_0$.
2. Let $\mathbb{S}_1^{k} = \binom{\mathcal{A}_1}{1} \| \binom{\mathcal{P}}{k-1}$, $\mathbb{S}_0^{k} = \binom{\mathcal{A}_0}{1} \| \binom{\mathcal{P}}{k-1}$, $\mathcal{H}_{k} = \mathcal{P}$, and $c_1^k = c_0^k = \emptyset$
3. If $\exists \rho \in \mathcal{R}(r)$ such that $\Pr\left[\max_{i\in[r]} \left| Y_i^{\mathbb{S}_1^{k+1}} - Y_i^{\mathbb{S}_0^{k+1}} \right| \geq \frac{\rho}{256\sqrt{r}}\right] \geq \frac{1}{2\rho\log(r)}$:
   (a) Set $\rho_k = \rho$.
   (b) For $\ell = k \ldots 2$:
   If $\exists z \in \{1,0\}$, $h, h' \in \mathcal{H}_\ell \setminus c_1^\ell \cup c_0^\ell$, $\rho \in \mathcal{R}(r)$ such that
   $$\Pr\left[\max_{i\in[r]} \left| Y_i^{\mathbb{S}_z^\ell(h)} - Y_i^{\mathbb{S}_z^\ell(h')} \right| \geq \frac{\rho}{256\sqrt{r}} \cdot \frac{\mathsf{coef}_n(k,\ell-1)^{1/2}}{(64\log(r))^{k-\ell+1}}\right] \geq \frac{1}{2\rho\log(r)} \cdot \frac{64^{-k+\ell-1}}{\mathsf{coef}_n(k,\ell-1)^{1/2}}$$
   define:
      i. $\mathbb{S}_1^{\ell-1} = \mathbb{S}_z^\ell(h)$, $\mathbb{S}_0^{\ell-1} = \mathbb{S}_z^\ell(h')$,
      ii. $\mathcal{H}_{\ell-1} = \mathcal{H}_\ell \setminus c_z^\ell$,
      iii. $c_1^{\ell-1} = \{h\}$ and $c_0^{\ell-1} = \{h'\}$,
      iv. $\rho_{\ell-1} = \rho$.
   Else, define $k^* = \ell$, $\rho^* = \rho_\ell$, $(\mathbb{S}_1, \mathbb{S}_0) = (\mathbb{S}_1^\ell, \mathbb{S}_0^\ell)$ and $\mathcal{H} = \mathcal{H}_{k^*} \setminus c_{k^*}^1 \cup c_{k^*}^0$.
   (c) If k^* was not assigned, set $k^* = 1$, $\rho^* = \rho_1$, $(\mathbb{S}_1, \mathbb{S}_0) = (\mathbb{S}_1^1, \mathbb{S}_0^1)$, and let $\mathcal{H} = \mathcal{A}_1$ if $\mathbb{S}_1$ and $\mathbb{S}_0$ are obtained as a concatenation of $\mathcal{A}_1$ with some other tuple set, and $\mathcal{H} = \mathcal{A}_0$ otherwise.

Else, let $k^* = k+1$, $\rho^* = 1$ and $(\mathbb{S}_1, \mathbb{S}_0, \mathcal{H}) = (\mathbb{S}_1^{k+1}, \mathbb{S}_0^{k+1}, \mathcal{H}_{k+1})$.

Figure 1: The Nugget

4 Augmented Weak Martingales have Large Gaps

In this section, we prove a generalization of the result of Cleve and Impagliazzo [11] who showed that (strong) martingales have large gap. Specifically, we prove a similar result for a sequence of non-strong martingales by identifying weaker requirements for the associated sequence to exhibit large gaps between consecutive points. We refer to such a sequence as *augmented weak martingales*. The reader is refereed to Section 1.1.1 for an informal discussion and motivation for the present section.

Consider a sequence $Z = (Z_1, \ldots, Z_r)$ of random variables over a domain $\mathcal{D}$, and a function f that takes as input a sequence of values $(z_1, \ldots, z_r)$ and returns a real value. We are interested in estimating $\mathbf{E}[f(Z)]$, given some partial information about $Z_{\leq i} = (Z_1, \ldots, Z_i)$ for $i \in [r]$. For

reasons discussed above, we wish to have this partial information informative enough to ensure a gap between the best estimation at i and the best estimation at $i+1$. On the other hand, we wish this partial information to be concise enough to allow us to efficiently estimate the expectation of $f(Z)$, conditioned on the partial information that we have. To this end, we consider a sequence of random variables $X_0, ..., X_r$, which we call the *Doob augmented weak martingales of* Z, describing the above expected value.

Below, we formally describe these random variables. Let us first give an overview of the way $X_0, ..., X_r$ are constructed by employing a short-output function χ describing the partial information we hold when estimating $f(Z)$. The sequence $X_0 \dots X_r$ resulting from the construction may be viewed as a sequence of "press releases" about $f(Z)$ given an aggregated account of the history of the Z's. $X_0 = \mathbf{E}[f(Z)]$ is just the expected value of $f(Z)$. The computation of X_i takes into account Z_i — the newly revealed point of the the Z-sequence — and $\chi_{i-1}(Z_{\leq i-1})$ — concise (partial) information about the Z-sequence up to, and including, point $i-1$. The concise $\chi_j(z_{\leq j})$ is computed by j recursive applications of χ, formally $\chi_j(z_{\leq j}) = \chi(j, z_j, \chi_{j-1}(z_{\leq j-1}))$. It is convenient to assume that $\chi_j(z_{\leq j})$ has X_j as its prefix, we then say that χ is normal form. Finally, X_i is a discretesized version (up to δ-long intervals) of the expected value of $f(Z)$, conditioned on Z_i and $\chi_{i-1}(z_{\leq i-1})$.

Definition 4.1 (The augmented weak martingale)**.** *Let $\delta \geq 0$, let $Z = (Z_1, \dots, Z_r)$ be a sequence of random variables, and let f and χ be functions. Define the following two functions for $i, i \in [r]$:*

- $\chi_j(z_{\leq j}) = \chi(j, z_j, \chi_{j-1}(z_{\leq j-1}))$*, letting* $\chi_0(\cdot) = \perp$*,*
- $\boldsymbol{x}_i(z_i, \mathsf{agt}_{i-1}) = \mathsf{rnd}_\delta(\mathbf{E}\left[f(Z_{\leq r}) \mid Z_i = z_i, \chi_{i-1}(Z_{\leq i-1}) = \mathsf{agt}_{i-1}\right])$ *(where $\boldsymbol{x}_i$ is a two-argument function and agt_{i-1} is a name of an argument).*

The Doob augmented weak martingales of (Z, f, χ, δ) is the sequence $X_0, ..., X_r$ defined by $X_0 = \mathbf{E}[f(Z)]$, and, for every $i \in [r]$,

$$X_i = \boldsymbol{x}_i(Z_i, \chi_{i-1}(Z_{\leq i-1})).$$

The function χ is in normal form*, if the output of $\chi(i, z_i, \mathsf{agt}_{i-1})$ is of the form $(x_i, \cdot)$, for $x_i = \boldsymbol{x}_i(z_i, \mathsf{agt}_{i-1})$. A normal form function χ* augments *a function g, if it is of the form $\chi(i, z_i, \mathsf{agt}_{i-1}) = (x_i, \cdot, g(z_i, x_i, \mathsf{aux}_{i-1}))$, when $\mathsf{agt}_{i-1} = (\cdot, \mathsf{aux}_{i-1})$.*

It is worth noting that specific choices for χ and δ yield familiar sequences. For example, if χ simply outputs its argument, i.e. $\chi_i(Z_{\leq i}) = Z_{\leq i}$, and $\delta = 0$, then we obtain the familiar Doob (strong) Martingale. On the other hand, if $\delta = 0$ and $\chi_i(Z_{\leq i}) = X_i$, i.e. χ is the minimal normal form function, then the construction yields the familiar Doob weak Martingale.

In the claim below, we show that the Doob augmented weak martingale of (Z, f, χ, δ) admits the 2δ-weak martingale property.

Lemma 4.2. *Let $X_0, ..., X_r$ be the Doob augmented weak martingale of (Z, f, χ, δ). Then $\mathbf{E}[X_{i+1} \mid X_i, \chi_i(Z_{\leq i})] \in X_i \pm 2\delta$ for every $i \in [r-1]$. In particular, $\mathbf{E}[X_{i+1} \mid X_i] \in X_i \pm 2\delta$, and if χ is normal form, then $\mathbf{E}[X_{i+1} \mid \chi_i(Z_{\leq i})] \in X_i \pm 2\delta$ for every $i \in [r-1]$.*

Proof. By Fact 2.9 and the definition of normal form, it suffices to prove the first part of the lemma. Let $X_0, ..., X_r$ be the Doob augmented weak martingale of (Z, f, χ, δ). Recall that $X_j =$

$\mathsf{rnd}_\delta(\mathbf{E}[f(Z) \mid Z_j, \chi_{j-1}(Z_{\leq j-1})])$ and let $\widetilde{X}_j = \mathbf{E}[f(Z) \mid Z_j, \chi_{j-1}(Z_{\leq j-1})]$ i.e., without rounding. Notice that

$$\begin{aligned}\mathbf{E}[X_{i+1} \mid X_i, \chi_i(Z_{\leq i})] &= \mathbf{E}\left[\mathsf{rnd}_\delta(\widetilde{X}_{i+1}) \mid X_i, \chi_i(Z_{\leq i})\right] \\ &\in \mathbf{E}\left[\widetilde{X}_{i+1} \mid X_i, \chi_i(Z_{\leq i})\right] \pm \delta\end{aligned}$$

Next, since both $\widetilde{X}_i$ and $\chi_i(Z_{\leq i})$ are functions of Z_i and $\chi_{i-1}(Z_{\leq i-1})$, it follows that, by Fact 2.11, $\mathbf{E}\left[\widetilde{X}_{i+1} \mid \widetilde{X}_i, \chi_i(Z_{\leq i})\right] = \widetilde{X}_i$. Consequently, by Fact 2.12, $\mathbf{E}\left[\widetilde{X}_{i+1} \mid X_i, \chi_i(Z_{\leq i})\right] \in X_i \pm \delta$ and thus $\mathbf{E}[X_{i+1} \mid X_i, \chi_i(Z_{\leq i})] \in X_i \pm 2\delta$. □

We are now ready to state the main theorem of the current section. The theorem asserts that for any sequence $Z = Z_1 \dots Z_r$ and function f such that $\mathbf{E}[f(Z)] = 1/2$ and $f(Z) \in \{0, 1\}$, there exists $\delta \geq 0$ and a normal-form function χ of output length that is logarithmic in $1/\delta$ and r such that the Doob augmented weak martingale of (Z, f, χ, δ) exhibits "large" gaps (of order $1/\sqrt{r}$) between consecutive points with constant probability. In addition, for any function g, this property is preserved for the Doob augmented weak martingale of (Z, f, χ^g, δ), where χ^g is a suitable function that augments g. What's more, the support of every X_i is of size $1/\delta$.

As mentioned above, the following theorem is a generalization of the of a theorem by Cleve and Impagliazzo [11], showing that (strong) martingales have large gap. More precisely, in [11], the authors proved the theorem for the Doob (strong) martingale of (Z, f), i.e. with $\chi_i(Z_{\leq i}) = Z_{\leq i}$ and $\delta = 0$. We stress that for the result of [11], the support of X_i and the image of χ may be potentially huge (exponential in r).

Theorem 4.3 (Augmented Weak Martingales have Large Gaps)**.** *For a sequence of random variables $Z = (Z_1, \dots, Z_r)$ a function f and $0 \leq \delta \leq 1/100r$, there exists a normal-form, $(\log r + 2\log 1/\delta + 1)$-bit output function χ such that the following holds for the Doob augmented weak martingale $X_0, \dots, X_r$ of (Z, f, χ, δ) (see Definition 4.1). If $\mathbf{E}[f(Z)] = 1/2$ and $f(Z_1, \dots, Z_r) \in \{0, 1\}$, then*

$$\Pr\left[\max_{i \in \{1,\dots,r\}} |X_i - X_{i-1}| > 1/32\sqrt{r}\right] \geq 1/5 \tag{23}$$

Furthermore, for any t-bit output g, there exists a normal-form, $(t + \log r + 2\log 1/\delta + 1)$-bit output function χ^g that augments g such that Equation (23) holds for the Doob augmented-weak martingale of (Z, f, χ^g, δ).

Remark 4.4 (Computing $X_0 \dots X_r$)**.** *Each X_i is fully determined by the index i, Z_i and the output of $\chi_{i-1}(Z_{\leq i})$. Since the latter is of size $(t + \log r + 2\log 1/\delta + 1)$, it follows that the sequence can be fully described using a table of size $\log(1/\delta) \cdot \max_i\{|\mathrm{supp}(Z_i)|\} \cdot 2^{t+1} \cdot (r/\delta)^2$. In particular, if $t = \Theta(\log(r))$, $1/\delta = \Theta(r)$ and $\max_i\{|\mathrm{supp}(Z_i)|\} = \Theta(r)$, it is immediate that the sequence $X_0 \dots X_r$ can be fully described by a string of size polynomial in r.*

The remainder of this section is dedicated to the proof of Theorem 4.3.

4.1 The Augmented Function

We begin by defining the augmented function. For δ, f and Z and an arbitrary auxiliary function g as in Theorem 4.3, we directly define the function $\chi^g = \chi^{\delta,f,g,Z}$ with respect to the function g. We remark that the definition of $\chi = \chi^{\delta,f,Z}$ is derived by taking g to be the empty (no output) function.

Notation 4.5. *For $x, x' \in [0,1]$ and $r \in \mathbb{N}$, let $\mathsf{gap}_r(x,x')$ be one if $|x - x'| \leq 1/32\sqrt{r}$ and zero otherwise, and let $\mathsf{mgap}_r(x,x') = \mathsf{gap}_r(x,x') \cdot (x - x')$.*

Definition 4.6 (The augmented function $\chi^{\delta,f,g,Z}$)**.** *Let $\delta > 0$, f and g be functions, and $Z = (Z_1, \ldots, Z_r)$ be a sequence of random variables. For $i \in [r]$, the output of $\chi^{\delta,f,g,Z}(i, z_i, \mathsf{agt}_{i-1} = (x_{i-1}, \mathsf{ng}_{i-1}, \mathsf{sg}_{i-1}, \mathsf{aux}_{i-1}))$ is defined as $(x_i, \mathsf{ng}_i, \mathsf{sg}_i, \mathsf{aux}_i)$ for*

- *Let $\chi_{i-1}(z_{\leq i-1}) = \chi^{\delta,f,g,Z}(i-1, z_{i-1}, \chi_{i-2}(z_{\leq i-2}))$ by letting $\chi_0(\emptyset) = (x_0, \mathsf{ng}_0, \mathsf{sg}_0, \mathsf{aux}_0) = (\mathbf{E}[f(Z)], 1, 0, g(\emptyset))$.*

- $x_i = \boldsymbol{x}_i(z_i, \mathsf{agt}_{i-1}) = \mathsf{rnd}_\delta\left(\mathbf{E}\left[f(Z_{\leq r}) \mid Z_i = z_i, \chi_{i-1}(Z_{\leq i-1}) = \mathsf{agt}_{i-1}\right]\right)$.

- $\mathsf{ng}_i = \mathsf{ng}_{i-1} \wedge \mathsf{gap}_r(x_i, x_{i-1})$, *letting gap_r be according to Notation 4.5.*

- $\mathsf{sg}_1 = \mathsf{rnd}_\delta\left(\mathbf{E}\left[\mathsf{mgap}_r(\boldsymbol{x}_1(Z_1, \chi_0(\emptyset)), \mathbf{E}[f(Z)])\right]\right)$,
  $\mathsf{sg}_i = \mathsf{sg}_{i-1} + \mathsf{rnd}_\delta\left(\mathbf{E}\left[\mathsf{mgap}_r(\boldsymbol{x}_i(Z_i, \chi_{i-1}(Z_{\leq i-1})), \boldsymbol{x}_{i-1}(Z_{i-1}, \chi_{i-2}(Z_{\leq i-2}))) \mid \chi_{i-1}(Z_{\leq i-1}) = \mathsf{agt}_{i-1}\right]\right)$,
  letting mgap_r be according to Notation 4.5.

- $\mathsf{aux}_i = g(z_i, \mathsf{agt}_{i-1})$.

For $(X_i, \mathsf{NG}_i, \mathsf{Sg}_i, \mathsf{Aux}_i) = \chi_i(Z_{\leq i})$, it holds that X_i is the expected value of f given Z_i and the information aggregated in $\chi_{i-1}(Z_{\leq i-1})$. The indicator NG_i tells us whether a big gap occured between consecutive X_j's, prior to the revelation of Z_i. Furthermore, Sg_i denotes the sum the the expected small gaps in the sequence, where the j^{th} summand is conditioned on the aggregated information before Z_j was sampled. Finally, Aux_i contains arbitrary auxiliary information about $Z_{\leq i}$.

The definition of NG_i and Sg_i might seem somewhat arbitrary, and indeed their exact formulation is dictated by the proof. Yet, as an informal motivation, note that $\mathsf{NG}_i = 0$ means a "jump" of $1/32\sqrt{r}$ between consecutive X_j's has occured. Similarly, "low" value of Sg_i means that a jump is likely to have occurred. Indeed, if Sg_i is always small then the last point of the martingale is unlikely to reach either 0 or 1. So we only need to make sure that the event $\mathsf{NG}_r = 1$ and Sg_r is large is not very likely. For the latter, we exploit the martingale property by pointing out that the j^{th} summand of Sg_r is equal to the expectation of the negation of $\mathsf{gap}_r(X_j, X_{j-1})$ (i.e. whether X_j and X_{j-1} are far by more than $1/32\sqrt{r}$). Thus, if Sg_r is large, then the same is true for $\sum_{j \leq r} \mathbf{E}[\neg\mathsf{gap}_r(X_j, X_{j-1}) \mid \ldots]$. In summary, if $\mathsf{NG}_r = \wedge_{j \leq r}\, \mathsf{gap}_r(X_j, X_{j-1}) = 1$ and $\sum_{j \leq r} \mathbf{E}[\neg\mathsf{gap}_r(X_j, X_{j-1}) \mid \ldots]$ is large, it means that no big gap occurred even though the sum of the expectations is large. We show, similarly to [11], the probability of that happening is far from 1 by a constant term.

The output-length of χ. By construction, the output length of $\chi^{\delta,f,g,Z}$ can be represented using $(t + \log r + 2\log(1/\delta) + 1)$ bits, assuming the output length of g is at most t.

4.1.1 The Augmented Function Yields Martingale Sequences with Large Gaps

Our proof follows the foot steps of [11]. The main difference (and difficulty) is to apply the (strong) martingale tools to sequences that are not necessarily strong martingales. We show that our sequences satisfy weaker variants of the martingale property and that these weaker conditions suffice for the sequence to have large gaps.

Notation 4.7. *Let $X_0 \dots X_r$ be as in Definition 4.6. For every $i \in [r]$, let $Y_i = X_i - X_{i-1}$, $W_i = \mathsf{gap}_r(X_i, X_{i-1})$, $S_i = \mathsf{mgap}_r(X_i, X_{i-1}) = W_i \cdot Y_i$, and $B_i = \mathsf{Sg}_i - \mathsf{Sg}_{i-1} = \mathsf{rnd}_\delta(\mathbf{E}\left[S_i \mid \chi^g_{i-1}(Z_{\le i-1})\right])$ letting $\delta \le 1/100r$. Finally, let $B'_i = S_i$ if $\wedge_{j\le i-1} W_j = \mathsf{NG}_{i-1} = 0$ and $B'_i = B_i$, otherwise. In plain terms, X_i denotes the augmented weak martingale sequence, Y_i denotes the difference-sequence and W_i denotes whether the i^{th} difference is small. Moreover, S_i is equal to Y_i when Y_i is small and 0 otherwise, and B_i denotes the expected value, rounded below, of S_i given $\chi^g(Z_{\le i-1})$. Finally write $\overline{W}_i = 1 - W_i$ for the negation of W_i.*

Theorem 4.3 immediately follows from the claims below.

Claim 4.8.
$\Pr[W_1 \wedge \ldots \wedge W_r] \le \Pr[|\sum_{i=1}^r S_i - B'_i| \ge 1/4] + \Pr[|\sum_{i=1}^r B_i| \ge 1/4 \wedge\ W_1 \wedge \ldots \wedge W_r]$.

Claim 4.9. $\Pr[|\sum_{i=1}^r S_i - B'_i| \ge 1/4] < 2 \cdot e^{-7}$.

Claim 4.10. $\Pr[|\sum_i B_i| \ge 1/4 \wedge\ W_1 \wedge \ldots \wedge W_r] < e^{-\frac{1}{4}+\frac{1}{100}}$.

Before we proving these claims, notice that

$$\Pr\left[\max_{i\in[r]} |X_i - X_{i-1}| \ge 1/32\sqrt{r}\right] \ge 1 - \Pr[W_1 \wedge \ldots \wedge W_r] \ge 1/5\ .$$

Furthermore, by construction, the output length of χ^g can be represented using $(t + \log r + 2\log(1/\delta) + 1)$ bits, assuming the output length of g is at most t. So, Theorem 4.3 follows immediately. □

Proving Claim 4.8 The claim follows from the hypothesis of the theorem and basic principles.

Proving Claim 4.8. From the hypothesis of Theorem 4.3, $\mathbf{E}[f(Z)] = 1/2$ and $f(Z) \in \{1, 0\}$. Thus, $|\sum_{i=1}^r Y_i| = |f(Z) - \mathbf{E}[f(Z)]| = 1/2$. Furthermore, $|\sum_{i=1}^r Y_i| \ge |\sum_{i=1}^r W_i \cdot Y_i - B'_i| + \left|\sum_{i=1}^r B'_i + \overline{W}_i \cdot Y_i\right|$. The calculation below concludes the proof.

$$\begin{aligned}
&\Pr[W_1 \wedge \ldots \wedge W_r] \\
&\quad= \Pr\left[W_1 \wedge \ldots \wedge W_r \wedge \left|\sum_i Y_i\right| \ge 1/2\right] \\
&\quad\le \Pr\left[W_1 \wedge \ldots \wedge W_r \wedge \left|\sum_i S_i - B'_i\right| \ge 1/4\right] + \Pr\left[\left|\sum_i B'_i + \overline{W}_i \cdot Y_i\right| \ge 1/4 \wedge\ W_1 \wedge \ldots \wedge W_r\right] \\
&\quad\le \Pr\left[\left|\sum_i S_i - B'_i\right| \ge 1/4\right] + \Pr\left[\left|\sum_i B_i\right| \ge 1/4 \wedge\ W_1 \wedge \ldots \wedge W_r\right].
\end{aligned}$$

□

Proving Claim 4.9 First we show that the gaps between the small increments (i.e. S_i's) and their rounded expectation (i.e. B_i's) form a δ-weak martingale difference sequence. Then, we show that the sequence is concentrated via the appropriate variant of Azuma's inequality.

Claim 4.11. *$= \{S_i - B'_i\}_{i=1}^r$ is a δ-weak martingale difference sequence.*

Proof. The proof follows from the construction of the sequence and a technical observations about conditional expectation (Fact 2.10). By Definition 2.14, we need to show that $\mathbf{E}\left[S_i - B'_i \mid \sum_{j<i} S_j - B'_j\right] \in \pm\delta$. By Fact 2.9, it suffices to show that $\mathbf{E}\left[S_i - B'_i \mid \sum_{j<i} S_j - B'_j, \bigwedge_{j<i} W_j\right] \in \pm\delta$. Recall that $B'_i = S_i$ whenever $\bigwedge_{j<i} W_j = 0$. Thus, for any $\sigma \in \mathrm{supp}(\sum_{j<i} S_j - B'_j)$,

$$\mathbf{E}\left[S_i - B'_i \mid \sum_{j<i} S_j - B'_j = \sigma, \bigwedge_{j<i} W_j = 0\right] = 0 \ .$$

On the other hand, let $\sigma \in \mathrm{supp}(\sum_{j<i} S_j - B'_j)$, and compute

$$\begin{aligned}
&\mathbf{E}\left[S_i - B'_i \mid \sum_{j<i} S_j - B'_j = \sigma, \bigwedge_{j<i} W_j = 1\right] \\
&\quad = \mathbf{E}\left[S_i - B_i \mid \sum_{j<i} Y_j - B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] = \mathbf{E}\left[S_i - B_i \mid X_{i-1} - \sum_{j<i} B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] \\
&\quad \in \mathbf{E}\left[S_i \mid X_{i-1} - \sum_{j} B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] \\
&\qquad - \mathbf{E}\left[\mathbf{E}\left[S_i \mid \chi^g_{i-1}(Z_{\le i-1})\right] \mid X_{i-1} - \sum_{j<i} B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] \pm \delta \qquad (24) \\
&\quad \in \mathbf{E}\left[S_i \mid X_{i-1} - \sum_{j<i} B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] - \mathbf{E}\left[S_i \mid X_{i-1} - \sum_{j<i} B_j = \sigma, \bigwedge_{j<i} W_j = 1\right] \pm \delta \qquad (25) \\
&\quad \in \pm\delta \ .
\end{aligned}$$

Equation (24) follows from the fact that B_i is δ-close to the relevant expectation. Equation (25) follows from Fact 2.10 by observing that $\chi^g_{i-1}(Z_{\le i-1})$ determines whether $X_{i-1} - \sum_{j-i} B_j = \sigma$ and $\bigwedge_{j<i} W_j = 1$. □

Proof Claim 4.9. It remains to bound $\sum_{i=0}^r S_i - B'_i$, where the underlying sequence is a δ-weak martingale difference sequence. Since $|S_i - B'_i| \le 1/16\sqrt{r} + \delta$, by Azuma's inequality for δ-weak

martingales, i.e. Theorem 2.16, it holds that

$$\begin{aligned}\Pr\left[\left|\sum_{i=0}^{r} S_i - B'_i\right| \geq \frac{1}{4}\right] &\leq 2 \cdot \exp\left(-\frac{1}{2} \cdot \left(\frac{1}{4} - r\delta\right)^2 \cdot \frac{1}{r \cdot (1/16\sqrt{r} + \delta)^2}\right) \\ &\leq 2 \cdot \exp\left(-\frac{1}{2} \cdot \left(\frac{1}{4} - \frac{1}{100}\right)^2 \cdot 16^2 \cdot \left(1 - \frac{1}{100}\right)\right) \\ &\leq 2 \cdot \exp\left(-7\right) \ .\end{aligned}$$

□

Proving Claim 4.10 Next, we bound the probability that the sum of the expectation of the small increments is large (greater than 1/4) while no big increment occurred. To this end, we exploit the martingale property by showing that the expectation of a small increment is δ-close to the expectation that a gap occurred. It then suffices to bound the probability that the sum of these expectations is large while none of those events occurred. More formally, we prove the claim by showing that $\mathbf{E}\left[\overline{W}_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \geq |B_i| - 2\delta$ and bounding the probability that $\sum_{i=1}^{r} \mathbf{E}\left[\overline{W}_i \mid \chi^g_{i-1}(Z_{\leq i})\right] \geq 1/4 - 2r\delta$ and $(\wedge_i W_i) = 1$.

Claim 4.12. *It holds that* $\mathbf{E}\left[\overline{W}_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \geq |B_i| - 2\delta$.

Proof. By the martingale property (c.f. Lemma 4.2),

$$\begin{aligned}&\mathbf{E}\left[\overline{W}_i \cdot Y_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] + \mathbf{E}\left[W_i \cdot Y_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \\ &\qquad = \mathbf{E}\left[Y_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \in \pm 2\delta \ .\end{aligned}$$

Thus, using the properties of expectation

$$\begin{aligned}\mathbf{E}\left[\overline{W}_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] &\geq \mathbf{E}\left[\overline{W}_i \cdot |Y_i| \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \\ &\geq \left|\mathbf{E}\left[\overline{W}_i \cdot Y_i \,|\, \chi^g_{i-1}(Z_{\leq i-1})\right]\right| \\ &\geq |B_i| - 2\delta \ .\end{aligned}$$

□

Proof of Claim 4.10. Let $A_i = \chi^g_i(Z_{\leq i})$, $\overline{D}_i = W_i$. By Fact 2.7, for any $\gamma \geq 0$, it holds that

$$\Pr\left[\sum_{i=1}^{r} \mathbf{E}\left[D_i \mid A_{i-1}\right] \geq \gamma \wedge \overline{D}_1 \wedge \ldots \wedge \overline{D}_r\right] \leq e^{-\gamma} \ .$$

Fix $\gamma = 1/4 - 2r\delta$ and deduce that

$$\begin{aligned}&\Pr\left[\left|\sum_i B_i\right| \geq 1/4 \wedge W_1 \wedge \ldots \wedge W_r\right] \\ &\qquad \leq \Pr\left[\sum_i \mathbf{E}\left[\overline{W}_i \mid \chi^g_{i-1}(Z_{\leq i-1})\right] \geq 1/4 - 2r\delta \wedge W_1 \wedge \ldots \wedge W_r\right] \\ &\qquad \leq e^{-1/4+2r\delta} \leq e^{-1/4+1/50}.\end{aligned}$$

□

5 Exploiting Similarity in Oblivious Sampling via Laplace Noise

Consider the following r-round game in which your goal is to maximize the revenue of a random "party" $H \leftarrow \mathcal{H}$. In the beginning, a party H is chosen with uniform distribution from $\mathcal{H}$ (where $\mathcal{H}$ is a finite set of parties). In each round, values $\left\{s_i^h \in [0,1]\right\}_{h\in\mathcal{H}}$ are assigned to the parties of $\mathcal{H}$, but only the values $\{s_h\}_{h\in\mathcal{H}\setminus\{H\}}$ of the other parties are published. You can decide to *abort*, and then party H is rewarded by s_i^H, or to continue to the next round. If an abort never occurs, party H is rewarded by s_r^H (last round value). You have the *similarity* guarantee that $\left|s_i^h - s_i\right| \leq \sigma$ for every $h \in \mathcal{H}$, letting $s_i = \mathbf{E}_{h\leftarrow\mathcal{H}}\left[s_i^h\right]$. You are also guarantee that $\max_i\{s_i\} \geq \gamma$.

In this section we analyze the following "differentially private based" approach for this task, which is described by the following experiment (the basic game described above is captured by the experiment for $p = 1/n$).

Experiment 5.1 (LapExp: Oblivious sampling experiment)**.**

Parameters: $\mathcal{H} = \{1,\ldots,n\}$, $\mathcal{S} = \left\{s_i^h \in [-1,1]\right\}_{i\in[r],h\in\mathcal{H}}$, $p \in [0,1/2]$, $\gamma \in [0,1]$ *and* $\lambda \in \mathbb{R}^+$.

Notation: Let $s_i = \frac{1}{n}\sum_{h\in\mathcal{H}} s_i^h$ *and for* $h \in \mathcal{H}$ *let* $s_i^{\setminus h} = \frac{1}{1-p}(s_i - p\cdot s_i^h)$.

Description:

1. *Sample* $h \leftarrow \mathcal{H}$.
2. *For* $i = 1,\ldots,r-1$*:*
   (a) *Sample* $\nu_i \leftarrow \mathsf{Lap}(\lambda)$.
   (b) *If* $s_i^{\setminus h} + \nu_i \geq \gamma$*, output* s_i^h *and halt.*
3. *Output* s_r^h.

Let $\mathsf{LapExp}(\mathcal{H},\mathcal{S},\gamma,\lambda)$ denote the above experiment with parameters $\mathcal{H}$, $\mathcal{S}$, γ and λ. Theorem 5.2 analyzes the expected value of the output of $\mathsf{LapExp}(\mathcal{H},\mathcal{S},\gamma,\lambda)$.

Theorem 5.2 (Quality of the oblivious sampling experiment)**.** *Let* $\mathcal{H}$*,* $\mathcal{S}$*,* γ*,* λ *and* p *be as in Experiment 5.1, with* $s_r^h = s_r$ *for every* $h \in \mathcal{H}$*. Let* $\sigma^h = \max_i\left\{\left|s_i - s_i^h\right|\right\}$*, let* $\mathcal{S}\mathsf{imilar} = \{h \in \mathcal{H}\colon \sigma_h \leq \lambda\cdot(1-p)/p\}$ *and* $\mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar} = \mathcal{H}\setminus\mathcal{S}\mathsf{imilar}$.

Let H *be the value of* h *and* J *be the halting round (set to* r *if Experiment 5.1 does not halt in step (2b)) in a random execution of* $\mathsf{LapExp}(\mathcal{H},\mathcal{S},\gamma,\lambda)$*. Then* $\mathbf{E}\left[s_J^H\right] \geq \mathbf{E}\left[v_H\right] - r\cdot e^{-\gamma/2\lambda}$*, where*

$$v_h = \begin{cases} \Pr\left[J \neq r \mid H = h\right]\cdot\left(\frac{\gamma}{2} - \frac{40(\sigma^h)^2}{\lambda}\cdot\frac{p}{1-p}\right), & h \in \mathcal{S}\mathsf{imilar}, \\ -4\sigma^h, & h \in \mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}. \end{cases}$$

If $\sigma_i \geq \gamma$ *for some* $i \in [r-1]$*, then* $\Pr\left[J \neq r \mid H = h\right]$ *is at least* $1/6$ *in the above expression.*

When using Theorem 5.2 in our proofs, the values $\mathcal{S} = \left\{s_i^h \in [-1,1]\right\}_{i\in[r],h\in\mathcal{H}}$ are calculated for a fixed transcript of the coin-flipping protocol. Corollary 5.3 analyse the expected value of the output when first a transcript τ is chosen, then the values $\mathcal{S}_\tau$ are computed, and finally $\mathsf{LapExp}(\mathcal{H},\mathcal{S}_\tau,\gamma,\lambda)$ is executed.

Corollary 5.3. *Let $\mathcal{H}$, γ, λ and p be as in Experiment 5.1. Let $\mathcal{S} = \left\{\mathcal{S}_\tau = \left\{s_i^h(\tau)\right\}_{i\in[r],h\in\mathcal{H}}\right\}_{\tau\in\mathcal{T}}$ denote a set of numbers in $[-1,1]$ indexed by $i \in [r]$, $h \in \mathcal{H}$ and τ taking values in some set $\mathcal{T}$. Define $\sigma^h(\tau) = \max_i\left\{\left|s_i(\tau) - s_i^h(\tau)\right|\right\}$. Let T be a random variable taking values in $\mathcal{T}$, and let H be the value of h and J be the halting round (set to r if Experiment 5.1 does not halt in step (2b)) in a random execution of $\mathsf{LapExp}(\mathcal{H}, \mathcal{S}_{\tau\leftarrow T}, \gamma, \lambda)$. Further assume that there exist real numbers α, β, γ, $\delta \in [0,1]$ such that*

- $\alpha \le \lambda(1-p)/2p$,
- $\Pr_{\tau\leftarrow T}\left[\sigma^h(\tau) \ge \rho\cdot\alpha\right] \le \frac{1}{\rho}\cdot\beta$, *for every* $h\in\mathcal{H}$ *and* $\rho \ge 1$,
- $\Pr_{\tau\leftarrow T}\left[\max_{i\in[r]} s_i(\tau) \ge \gamma\right] \ge \delta$.

Then,

$$\mathbf{E}\left[s_J^H(T)\right] \ge \frac{1}{6}\cdot(\delta-\beta/2)\cdot\left(\frac{\gamma}{2} - \frac{40\cdot\alpha^2 p}{\lambda(1-p)}\right) - 168\alpha\beta - 8\alpha\beta\log(1/\lambda) - \frac{r}{2}\cdot e^{-\gamma/2\lambda} \ .$$

In particular, if $\gamma \ge \frac{1}{256\sqrt{r}}$, $\lambda = \gamma/(4\log(r))$, $\alpha \le \frac{\gamma\sqrt{4(1-p)/p}}{32\log(r)}$ and $\beta \le \frac{\delta}{16\sqrt{(1-p)/p}}$, then $\mathbf{E}\left[s_J^H(T)\right] \ge \gamma\delta/64 - \frac{1}{2r}$, for r large enough.

5.1 Proving Theorem 5.2

Proof of Theorem 5.2. For $h\in\mathcal{H}$ and $i\in[r]$, let $d_i^h = s_i^{\setminus h} - s_i^h$. We next compute $\mathbf{E}\left[s_J^H\right]$.

$$\begin{aligned}
\mathbf{E}\left[s_J^H\right] &= \sum_{i\in[r],h\in\mathcal{H}} s_i^h\cdot\Pr\left[H=h\wedge J=i\right] \qquad (26)\\
&= \sum_{i,h}(s_i^{\setminus h} - d_i^h)\cdot\Pr\left[H=h\wedge J=i\right]\\
&= \sum_{i,h} s_i^{\setminus h}\cdot\Pr\left[H=h\wedge J=i\right] - \sum_{i,h} d_i^h\cdot\Pr\left[H=h\wedge J=i\right]\\
&= \mathbf{E}\left[s_J^{\setminus H}\right] - \sum_{i,h} d_i^h\cdot\Pr\left[H=h\wedge J=i\right]\\
&= \mathbf{E}\left[s_J^{\setminus H}\right] - \frac{1}{n}\cdot\sum_{i\in[r],h\in h} d_i^h\cdot\Pr\left[J=i\mid H=h\right]\\
&= \mathbf{E}\left[s_J^{\setminus H}\right] - \frac{1}{n}\cdot\sum_{i\in[r-1],h\in h} d_i^h\cdot\Pr\left[J=i\mid H=h\right].
\end{aligned}$$

The last equality holds since, by assumption, $s_r = s_r^h$ for any h, thus, $d_r^h = 0$.

We start by upper bounding the right hand term above (i.e., $\sum_{i,h} d_i^h\cdot\Pr\left[J=i\mid H=h\right]$). For $h\in\mathcal{H}$ and $i\in[r-1]$, let

$$p_i^h = \Pr\left[\mathsf{Lap}(\lambda) + s_i^{\setminus h} \ge \gamma\right],\ p_r^h = 1,\ \text{and}\ q_i^h = p_i^h\cdot\prod_{j<i}(1-p_j^h).$$

Note that $q_i^h = \Pr[J = i \mid H = h]$. For $i \in [r]$, let

$$p_i = \Pr[\mathsf{Lap}(\lambda) + s_i \geq \gamma] \text{ and } q_i = p_i \cdot \prod_{j<i}(1-p_j).$$

Let $\sigma_i^h = s_i - s_i^h$ and $\sigma_i^{\setminus h} = s_i - s_i^{\setminus h}$. Note that $d_i^h = -\sigma_i^{\setminus h} + \sigma_i^h$. Since $s_i = (1-p)\cdot s_i^{\setminus h} + p \cdot s_i^h$, it holds that $\sigma_i^{\setminus h} = -p \cdot \sigma_i^h/(1-p)$. In particular, for any $h \in \mathcal{S}\mathsf{imilar}$ it holds that $\left|\sigma_i^h\right| \leq \sigma_i^h \leq \lambda(1-p)/p$ and $\left|\sigma_i^{\setminus h}\right| \leq \lambda$. Hence, Fact 2.5 yields that $p_i^h/p_i \in 1 \pm 5\sigma^{\setminus h}/\lambda$ for any $h \in \mathcal{S}\mathsf{imilar}$. Therefore, by Lemma 2.6

$$\sum_{i\in[r-1]} \left|q_i - q_i^h\right| \leq \frac{20}{\lambda} \cdot \sigma^{\setminus h} \cdot (1-q_r^h) \leq \frac{20p}{\lambda(1-p)} \cdot \sigma^h \cdot (1-q_r^h) \tag{27}$$

for any $h \in \mathcal{S}\mathsf{imilar}$. Define $d^h = \max_i\left\{\left|d_i^h\right|\right\}$. It follows that

$$\begin{aligned}
\sum_{i\in[r-1],h\in\mathcal{H}} d_i^h \cdot \Pr[J = i \mid H = h] &= \sum_{i,h} d_i^h \cdot q_i^h \\
&= \sum_{i,h} d_i^h \cdot q_i + \sum_{i,h} d_i^h \cdot (q_i^h - q_i) \\
&= \sum_{i,h} d_i^h \cdot (q_i^h - q_i) \\
&\leq \sum_{h\in\mathcal{S}\mathsf{imilar}} d^h \sum_{i\in[r-1]} \left|q_i^h - q_i\right| + \sum_{h\in\mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}} 2d^h \\
&\leq \frac{20p}{\lambda\cdot(1-p)} \cdot \sum_{h\in\mathcal{S}\mathsf{imilar}} d^h \cdot \sigma^h \cdot (1-q_r^h) + \sum_{h\in\mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}} 2d^h \\
&\leq \frac{20p}{\lambda\cdot(1-p)} \cdot \sum_{h\in\mathcal{S}\mathsf{imilar}} 2(\sigma^h)^2 \cdot (1-q_r^h) + \sum_{h\in\mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}} 4\sigma^h.
\end{aligned} \tag{28}$$

The second equality holds since $\sum_{h\in\mathcal{H}} \sigma_i^h = 0$ for any $i \in [r]$, and thus $\sum_{h\in\mathcal{H}} \sigma_i^{\setminus h} = 0$ and $\sum_{h\in\mathcal{H}} d_i^h = 0$. The last inequality holds since $p \leq 1/2$ and thus $d^h = |-p\sigma^h/(1-p) - \sigma^h| \leq 2\sigma^h$.

The next step is to lower bound $\mathbf{E}\left[s_J^{\setminus H}\right]$. By Fact 2.4,

$$\Pr\left[J \neq r \wedge s_J^{\setminus H} \leq \gamma/2\right] = \sum_{i=1}^{r-1} \Pr\left[J = i \wedge s_J^{\setminus H} \leq \gamma/2\right] \leq \frac{r}{2} \cdot e^{-\gamma/2\lambda}. \tag{29}$$

Hence,

$$\begin{aligned}
\mathbf{E}\left[s_J^{\setminus H}\right] &\geq \Pr[J \neq r] \cdot \gamma/2 - \frac{r}{2} \cdot e^{-\gamma/2\lambda} \\
&= \mathbf{E}\left[1 - q_r^H\right] \cdot \gamma/2 - \frac{r}{2} \cdot e^{-\gamma/2\lambda} \\
&\geq \left(\frac{1}{n} \sum_{h\in\mathcal{S}\mathsf{imilar}} (1-q_r^h) \cdot \gamma/2\right) - \frac{r}{2} \cdot e^{-\gamma/2\lambda}.
\end{aligned} \tag{30}$$

It follows that

$$\begin{aligned}&\mathbf{E}\left[s_J^H\right] \\ &\geq \frac{1}{n}\left(\sum_{h\in\mathcal{S}\mathsf{imilar}}(1-q_r^h)\cdot\left(\gamma/2-\frac{40}{\lambda\cdot(1-p)/p}(\sigma^h)^2\right)\right)-\frac{1}{n}\sum_{h\in\mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}}4\sigma^h-\frac{r}{2}\cdot e^{-\gamma/2\lambda}.\end{aligned} \tag{31}$$

To conclude the proof we need to show that if $s_i \geq \gamma$ for some $i \in [r-1]$, then $(1-q_r^h) \geq 1/6$ for all $h \in \mathcal{S}\mathsf{imilar}$. Let $i \in [r-1]$ be a round with $s_i \geq \gamma$. For every $h \in \mathcal{S}\mathsf{imilar}$, we have shown that $\left|\sigma_i^{\setminus h}\right| \leq \lambda$, thus, $s_i^{\setminus h} \geq \gamma - \lambda$. By Fact 2.4, it holds that $p_i^h \geq \Pr\left[\mathsf{Lap}(\lambda) \geq \lambda\right] = \exp(-1)/2 \geq 1/6$. Hence, $1 - q_r^h \geq 1/6$, for all $h \in \mathcal{S}\mathsf{imilar}$. □

5.2 Proving Corollary 5.3

Before proving the theorem, we state and prove two claims regarding the expectation of the similarity gap.

Claim 5.4. *Under the hypothesis of Corollary 5.3, it holds that*

$$\mathbf{E}\left[\sigma^h(T)\,|\,\sigma^h(T)\geq(1-p)\lambda/p\right]\cdot\Pr\left[\sigma^h(T)\geq(1-p)\lambda/p\right]\leq 2\alpha\beta\log(1/\lambda)+2\alpha\beta\ , \tag{32}$$

$$\mathbf{E}\left[(\sigma^h(T))^2\,|\,\sigma^h(T)\in[\alpha,(1-p)\lambda/p]\right]\cdot\Pr\left[\sigma^h(T)\in[\alpha,(1-p)\lambda/p]\right]\leq 4(1-p)\lambda\alpha\beta/p\ . \tag{33}$$

for every $h \in \mathcal{H}$.

Proof. We begin by showing (32).

$$\begin{aligned}&\mathbf{E}\left[\sigma^h(T)\,|\,\sigma^h(T)\geq(1-p)\lambda/p\right]\cdot\Pr\left[\sigma^h(T)\geq(1-p)\lambda/p\right] \\ &\qquad\leq\sum_{i=\log((1-p)\lambda/p\alpha)}^{\log(1/\alpha)}\alpha 2^{i+1}\cdot\Pr\left[\sigma^h(T)\in\alpha\cdot[2^i,2^{i+1}]\right] \\ &\qquad\leq\sum_{i=\log((1-p)\lambda/p\alpha)}^{\log(1/\alpha)}\alpha 2^{i+1}\cdot\Pr\left[\sigma^h(T)\geq 2^i\cdot\alpha\right] \\ &\qquad\leq\sum_{i=\log((1-p)\lambda/p\alpha)}^{\log(1/\alpha)}\alpha 2^{i+1}\cdot 2^{-i}\beta \\ &\qquad=2\alpha\beta\left(\log(1/\alpha)-\log((1-p)\lambda/p\alpha)+1\right) \\ &\qquad=2\alpha\beta\log(p/(1-p)\lambda)+2\alpha\beta\leq 2\alpha\beta\log(1/\lambda)+2\alpha\beta\ .\end{aligned}$$

Next, we show (33).

$$\begin{aligned}
\mathbf{E}\left[(\sigma^h(T))^2 \,|\, \sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \cdot \Pr\left[\sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] & \\
&\leq \sum_{i=0}^{\log((1-p)\lambda/p\alpha)-1} \alpha^2 2^{2i+2} \cdot \Pr\left[\sigma^h(T) \in \alpha \cdot [2^i, 2^{i+1}]\right] \\
&\leq \sum_{i=0}^{\log((1-p)\lambda/p\alpha)-1} \alpha^2 2^{2i+2} \cdot 2^{-i} \cdot \beta \\
&= 4\alpha^2\beta \sum_{i=0}^{\log((1-p)\lambda/p\alpha)-1} 2^i \\
&= 4\alpha^2\beta((1-p)\lambda/p\alpha - 1) \leq 4\alpha\beta(1-p)\lambda/p \ .
\end{aligned}$$

□

Proof of Corollary 5.3. To prove the claim, we will combine Theorem 5.2 with (32) and (33) from Claim 5.4. Using the notation from Theorem 5.2, we compute

$$\begin{aligned}
\mathbf{E}[v_h] = \mathbf{E}\left[v_h \,|\, \sigma^h(T) \leq \alpha\right] \cdot \Pr\left[\sigma^h(T) \leq \alpha\right] & \\
+ \mathbf{E}\left[v_h \,|\, \sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \cdot \Pr\left[\sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] & \\
+ \mathbf{E}\left[v_h \,|\, \sigma^h(T) \geq (1-p)\lambda/p\right] \cdot \Pr\left[\sigma^h(T) \geq (1-p)\lambda/p\right] \ . &
\end{aligned}$$

We compute each of these terms separately. First, by the definition of v_h in Theorem 5.2,

$$\mathbf{E}\left[v_h \,|\, \sigma^h(T) \leq \alpha\right] \cdot \Pr\left[\sigma^h(T) \leq \alpha\right] \geq \left(\frac{\gamma}{2} - \frac{40 \cdot \alpha^2}{\lambda(1-p)/p}\right) \cdot \Pr\left[J \neq r \ \wedge \ \sigma^h(T) \leq \alpha\right] \ .$$

Next,

$$\begin{aligned}
\mathbf{E}\left[v_h \,|\, \sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \cdot \Pr\left[\sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \geq & \\
\frac{\gamma}{2} \cdot \Pr\left[J \neq r \ \wedge \ \sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] & \\
- \frac{40}{(1-p)\lambda/p} \cdot \mathbf{E}\left[(\sigma^h(T))^2 \,|\, \sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \cdot \Pr\left[\sigma^h(T) \in [\alpha, (1-p)\lambda/p]\right] \ . &
\end{aligned}$$

Finally,

$$\begin{aligned}
\mathbf{E}\left[v_h \,|\, \sigma^h(T) \geq (1-p)\lambda/p\right] \cdot \Pr\left[\sigma^h(T) \geq (1-p)\lambda/p\right] \geq & \\
- 4 \cdot \mathbf{E}\left[\sigma^h(T) \,|\, \sigma^h(T) \geq (1-p)\lambda/p\right] \cdot \Pr\left[\sigma^h(T) \geq (1-p)\lambda/p\right] \ . &
\end{aligned}$$

Add the three terms together and replace the relevant expressions using (32) and (33):

$$\mathbf{E}[v_h] \geq \Pr[h \in \mathcal{S}\mathsf{imilar} \wedge J \neq r] \cdot \left(\frac{\gamma}{2} - \frac{40 \cdot \alpha^2}{(1-p)\lambda/p}\right) - 40 \cdot 4\alpha\beta - 8\alpha\beta\log(1/\lambda) - 8\alpha\beta \ .$$

Next, we lower-bound the quantity $\Pr[h \in \mathcal{S}\mathsf{imilar} \wedge J \neq r]$.

$$\begin{aligned}\Pr[h \in \mathcal{S}\mathsf{imilar} \wedge J \neq r] &\geq \Pr[h \in \mathcal{S}\mathsf{imilar} \wedge J \neq r \wedge \exists s_i(T) \geq \gamma] \\ &= \Pr[J \neq r \mid h \in \mathcal{S}\mathsf{imilar} \wedge \exists s_i(T) \geq \gamma] \cdot \Pr[h \in \mathcal{S}\mathsf{imilar} \wedge \exists s_i(T) \geq \gamma] \\ &\geq \frac{1}{6} \cdot (\Pr[\exists s_i(T) \geq \gamma] - \Pr[h \in \mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}]) \ .\end{aligned}$$

We conclude by observing that $\Pr[h \in \mathcal{N}\mathsf{on}\mathcal{S}\mathsf{imilar}] \leq \Pr\left[\sigma^h \geq 2\alpha\right] \leq \beta/2$.

The last part of the claim follows from the inequalities below. For r large enough,

$$\begin{aligned}&\delta - \frac{\beta}{2} \geq \frac{3\delta}{4} \\ &\frac{\gamma}{2} - \frac{40\alpha^2 p}{\lambda(1-p)} \geq \frac{\gamma}{4} \\ &168\alpha\beta + 8\alpha\beta\log(1/\lambda) \leq 8\alpha\beta\log(r) \\ &4\alpha\beta\log(r) \leq \frac{\gamma\delta}{64}\end{aligned}$$

□

References

[1] B. Alon and E. Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. In *Proceedings of the 14th Theory of Cryptography Conference, TCC 2016-B, part I*, pages 307–335, 2016.

[2] G. Asharov. Towards characterizing complete fairness in secure two-party computation. In Y. Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 291–316. Springer, 2014.

[3] G. Asharov, Y. Lindell, and T. Rabin. A full characterization of functions that imply fair coin tossing and ramifications to fairness. In A. Sahai, editor, *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013*, volume 7785 of *Lecture Notes in Computer Science*, pages 243–262. Springer, 2013.

[4] G. Asharov, A. Beimel, N. Makriyannis, and E. Omri. Complete characterization of fairness in secure two-party computation of boolean functions. In Y. Dodis and J. B. Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, 2015, Proceedings, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 199–228. Springer, 2015.

[5] B. Awerbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. How to implement Bracha's $O(\log n)$ byzantine agreement algorithm. Unpublished manuscript, 1985.

[6] A. Beimel, Y. Lindell, E. Omri, and I. Orlov. $1/p$-secure multiparty computation without honest majority and the best of both worlds. In P. Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 277–296. Springer, 2011.

[7] A. Beimel, E. Omri, and I. Orlov. Protocols for multiparty coin toss with a dishonest majority. *Journal of Cryptology*, 28(3):551–600, 2015.

[8] M. Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1983.

[9] N. Buchbinder, I. Haitner, N. Levi, and E. Tsfadia. Fair coin flipping: Tighter analysis and the many-party case. In *Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2580–2600, 2017.

[10] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC)*, pages 364–369, 1986.

[11] R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes (extended abstract). `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.51.1797`, 1993.

[12] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. On the black-box complexity of optimally-fair coin tossing. In *Proceedings of the 8th Theory of Cryptography Conference, TCC 2011*, volume 6597, pages 450–467, 2011.

[13] D. Dachman-Soled, M. Mahmoody, and T. Malkin. Can optimally-fair coin tossing be based on one-way functions? In Y. Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 217–239. Springer, 2014.

[14] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(34):211–407, 2014.

[15] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3):2, 2016.

[16] C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth. Guilt-free data reuse. *Commun. ACM*, 60(4):86–93, 2017.

[17] D. Gordon and J. Katz. Complete fairness in multi-party computation without an honest majority. In *Proceedings of the 6th Theory of Cryptography Conference, TCC 2009*, pages 19–35, 2009.

[18] D. Gordon and J. Katz. Partial fairness in secure two-party computation. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 157–176. Springer, 2010.

[19] S. D. Gordon, C. Hazay, J. Katz, and Y. Lindell. Complete fairness in secure two-party computation. *J. ACM*, 58(6):24:1–24:37, 2011.

[20] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2014.

[21] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. *SIAM J. Comput.*, 46(2):479–542, 2017.

[22] N. Makriyannis. On the classification of finite boolean functions up to fairness. In M. Abdalla and R. D. Prisco, editors, *Security and Cryptography for Networks - 9th International Conference, SCN 2014, 2014.*, volume 8642 of *Lecture Notes in Computer Science*, pages 135–154. Springer, 2014.

[23] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. In *Proceedings of the 6th Theory of Cryptography Conference, TCC 2009*, pages 1–18, 2009.

[24] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. *Journal of Cryptology*, 29(3): 491–513, 2016.

[25] P. I. Nelson. A class of orthogonal series related to martingales. *Annals of Mathematical Statistics*, 41:1684–1694, 1970.

A Missing Proofs

Proof of Fact 2.5. We distinguish four cases, depending on the signs of γ and γ'.

Case 1. $(\gamma \geq 0, \gamma' \geq 0)$**.** $p/p' = \frac{\frac{1}{2}\cdot e^{-\gamma}}{\frac{1}{2}\cdot e^{-\gamma+\varepsilon}} = e^{-\varepsilon} \in 1 \pm 2\varepsilon$.

Case 2. $(\gamma \geq 0, \gamma' < 0)$**.** $p/p' = \frac{\frac{1}{2}\cdot e^{-\gamma}}{1-\frac{1}{2}\cdot e^{\gamma-\varepsilon}} = \frac{1}{2e^{\gamma}-e^{2\gamma-\varepsilon}}$. Since $\gamma \geq 0$ and $\gamma - \varepsilon < 0$, it follows that $0 \leq \gamma \leq \varepsilon < 1$ and thus $-\varepsilon < \gamma - \varepsilon < \varepsilon$. Thus $\frac{1}{2e^{\gamma}-e^{2\gamma-\varepsilon}} = e^{-\varepsilon} \cdot \frac{1}{2e^{\gamma-\varepsilon}-e^{2(\gamma-\varepsilon)}} \in e^{\varepsilon} \cdot (1 \pm \varepsilon^2) \in 1 \pm 5\varepsilon$.

Case 3. $(\gamma < 0, \gamma' \geq 0)$**.** $p/p' = \frac{1-\frac{1}{2}\cdot e^{\gamma}}{\frac{1}{2}\cdot e^{-\gamma+\varepsilon}} = 2 \cdot e^{\gamma-\varepsilon} - e^{2\gamma-\varepsilon}$. Similarly to the previous case, since $\gamma < 0$ and $\gamma - \varepsilon \geq 0$, it follows that $0 > \gamma \geq \varepsilon > -1$ and thus $\varepsilon < \gamma < -\varepsilon$. Thus $2 \cdot e^{\gamma-\varepsilon} - e^{2\gamma-\varepsilon} = e^{-\varepsilon} \cdot (2e^{\gamma} - e^{2\gamma}) \in e^{-\varepsilon} \cdot (1 \pm \varepsilon^2) \in 1 \pm 5\varepsilon$.

Case 4. $(\gamma < 0, \gamma' < 0)$**:** $p/p' = \frac{1-\frac{1}{2}\cdot e^{\gamma}}{1-\frac{1}{2}\cdot e^{\gamma-\varepsilon}} = \frac{1-\frac{1}{2}\cdot e^{\gamma'-\varepsilon'}}{1-\frac{1}{2}\cdot e^{\gamma'}} = \frac{1-\frac{1}{2}\cdot e^{\gamma'}\cdot e^{-\varepsilon'}}{1-\frac{1}{2}\cdot e^{\gamma'}}$. Let $\mu = 1 - \frac{1}{2} \cdot e^{-\gamma'}$ and notice that $\mu \in [1/2, 1]$. Compute $\frac{1-\frac{1}{2}\cdot e^{\gamma'-\varepsilon'}}{\mu} = 1 + \frac{1-\mu}{\mu} - \frac{1-\mu}{\mu} \cdot e^{-\varepsilon'} \in 1 + \frac{1-\mu}{\mu} - \frac{1-\mu}{\mu} \cdot (1 \pm 2\varepsilon) \in 1 \pm 2\varepsilon$. □

Lemma A.1. *Consider an iterative sequence of r independent Bernoulli trials, where the success probability of the i^{th} trial is $p_i \in [0,1]$. Assume that $p_r = 1$. For $i \in [r]$, let $q_i = p_i \cdot \prod_{j<i}(1-p_j)$ be the probability of the first success occurring in the i^{th} trial. It holds that $\sum_{i=1}^{r} q_i \cdot (\sum_{j \leq i} p_j) = 1$.*

Proof. We prove the claim by proving a stronger statement. Namely, for arbitrary $p_r \in [0,1]$, we show that

$$\sum_{i=1}^{r} q_i \left(\sum_{j \leq i} p_j \right) = 1 - \left(\prod_{i \leq r} (1-p_i) \right) \left(1 + \sum_{i \leq r} p_i \right) \quad . \tag{34}$$

Notice that our claim is a special case of Equation (34) for $p_r = 1$. We proceed to prove the equation by induction on r. For $r = 1$, take arbitrary $p_1 \in [0,1]$ and notice that $q_1 p_1 = 1 - (1-p_1)(1+p_1)$.

Next, assume that Equation (34) is true and let $p_{r+1} \in [0,1]$. The calculation below concludes the proof.

$$\begin{aligned}\sum_{i=1}^{r+1} q_i \left(\sum_{j\le i} p_j\right) &= 1 - \left(\prod_{i\le r}(1-p_i)\right)\left(1+\sum_{i\le r} p_i\right) + p_{r+1}\left(\prod_{i\le r}(1-p_i)\right)\left(p_{r+1}+\sum_{i\le r} p_i\right)\\ &= 1 - \left(\prod_{i\le r}(1-p_i)\right)\left(1-p_{r+1}^2+(1-p_{r+1})\sum_{i\le r} p_i\right)\\ &= 1 - \left(\prod_{i\le r+1}(1-p_i)\right)\left(1+\sum_{i\le r+1} p_i\right),\end{aligned}$$

where the last transition follows using $1-p_{r+1}^2 = (1-p_{r+1})(1+p_{r+1})$. □

Lemma A.2. *Consider two iterative sequences, each of r independent Bernoulli trials. Let $p_i, p'_i \in [0,1]$ denote the success probability of the i^{th} trial of the first and second sequence, respectively. Assume that $p_r = p'_r = 1$. Let ε be such that for all $i \in [r]$, it holds that $\frac{p_i}{p'_i}, \frac{p'_i}{p_i}, \frac{(1-p'_i)}{(1-p_i)}, \frac{(1-p_i)}{(1-p'_i)} \in (1\pm\varepsilon)$. Then, for every $i \in [r]$,*

$$\left|\prod_{j\le i}(1-p'_j) - \prod_{j\le i}(1-p_j)\right| \le 3\varepsilon\left(\prod_{j\le i}(1-\min(p_j,p'_j))\right)\left(\sum_{j\le i}\min(p_j,p'_j)\right) \quad . \tag{35}$$

Proof. First, observe that $1-p_i \in (1\pm 3\varepsilon\cdot p_i)(1-p'_i)$ and $1-p'_i \in (1\pm 3\varepsilon\cdot p'_i)(1-p_i)$, for every $i\in[r]$. We hint on how to verify the former (the latter is symmetric). If $p_i \ge 1/3$ or if $p'_i \le 2/3$, then verifying $1-p_i \in (1\pm 3\varepsilon\cdot p_i)(1-p'_i)$ is easy. Otherwise, if $p_i < 1/3$ and $p'_i > 2/3$, then $\varepsilon p_i > 1/3$, and hence $3\varepsilon p_i > 1$. Thus, $(1\pm 3\varepsilon\cdot p_i)(1-p'_i) > 1 > 1-p_i$.

We prove Equation (35) by induction on i. For every $j\in[i]$, let $\widetilde{p}_j = \min(p_j,p'_j)$. For the base case, $|(1-p_1)-(1+p'_1)| \le 2\varepsilon\widetilde{p}_1(1-\widetilde{p}_1)$. Next, assume that Equation (35) is true up to some $i\in[r]$. Without loss of generality, further assume that $\widetilde{p}_{i+1} = p_{i+1}$ and let $u\in[0,1]$ such that $1-p_{i+1} = (1+3u\varepsilon p_{i+1})(1-p'_{i+1})$. For the induction step, compute

$$\begin{aligned}\left|\prod_{j\le i+1}(1-p'_j) - \prod_{j\le i+1}(1-p_j)\right| &\le (1-p'_{i+1})\left|\prod_{j\le i}(1-p'_j) - (1+3\varepsilon u p_{i+1})\prod_{j\le i}(1-p_j)\right|\\ &\le (1-p'_{i+1})\left|\prod_{j\le i}(1-p'_j) - \prod_{j\le i}(1-p_j)\right| + \left|3u\varepsilon p_{i+1}(1-p'_{i+1})\prod_{j\le i}(1-p_j)\right|\\ &\le (1-\widetilde{p}_{i+1})3\varepsilon\left(\prod_{j\le i}(1-\widetilde{p}_j)\right)\left(\sum_{j\le i}\widetilde{p}_j\right) + 3\varepsilon p_{i+1}\prod_{j\le i+1}(1-\widetilde{p}_j)\\ &= 3\varepsilon\left(\prod_{j\le i+1}(1-\widetilde{p}_j)\right)\left(\widetilde{p}_{i+1}+\sum_{j\le i}\widetilde{p}_j\right) \quad .\end{aligned}$$

The second inequality is by the triangle inequality. The third inequality follows by the induction hypothesis and the fact that for every $j \in [i+1]$ it holds that $1-p_j, 1-p'_j \leq 1-\widetilde{p}_j$. The last transition is true by the assumption that $\widetilde{p}_{i+1} = p_{i+1}$. □

Lemma A.3. *Consider two iterative sequences, each of r independent Bernoulli trials. Let $p_i, p'_i \in [0,1]$ denote the success probability of the i^{th} trial of the first and second sequence, respectively. Assume that $p_r = p'_r = 1$. For $i \in [r]$, let $q_i = p_i \cdot \prod_{j<i}(1-p_j)$ and $q'_i = p'_i \cdot \prod_{j<i}(1-p'_j)$. Let ε be such that for all $i \in [r]$, it holds that $\frac{p_i}{p'_i}, \frac{p'_i}{p_i}, \frac{(1-p'_i)}{(1-p_i)}, \frac{(1-p_i)}{(1-p'_i)} \in (1 \pm \varepsilon)$. Then, for every $i \in [r]$, it holds that*

$$\left|q_i - q'_i\right| \leq 3\varepsilon \cdot \min(p_i, p'_i) \cdot \left(\prod_{j<i}(1 - \min(p_j, p'_j))\right)\left(\frac{1}{3} + \sum_{j \leq i} \min(p_j, p'_j)\right) \quad . \tag{36}$$

Proof. For every $j \in [i]$, let $\widetilde{p}_j = \min(p_j, p'_j)$. Without loss of generality, assume that $\widetilde{p}_i = p_i$ and let $u \in [0,1]$ such that $p'_i = (1+u\varepsilon)p_i$ (there exists such u since $p'_i \in p_i(1 \pm \varepsilon)$).

$$\begin{aligned}
\left|p_i \prod_{j<i}(1-p_j) - p'_i \prod_{j<i}(1-p'_j)\right| &\leq p_i \left|\prod_{j<i}(1-p_j) - \prod_{j<i}(1-p'_j)\right| + \left|\varepsilon u p_i \prod_{j<i}(1-p'_j)\right| \\
&\leq 3\varepsilon\widetilde{p}_i \left(\prod_{j<i}(1-\widetilde{p}_j)\right)\left(\sum_{j<i}\widetilde{p}_j\right) + \varepsilon\widetilde{p}_i \prod_{j<i}(1-\widetilde{p}_j) \\
&\leq 3\varepsilon\widetilde{p}_i \left(\prod_{j<i}(1-\widetilde{p}_j)\right)\left(\frac{1}{3} + \sum_{j<i}\widetilde{p}_j\right) \quad .
\end{aligned}$$

The first inequality is by the triangle inequality. The second inequality follows by Lemma A.2 and the fact that for every $j \in [i]$ it holds that $1-p'_j \leq 1-\widetilde{p}_j$. □

Lemma A.4 (Restating Lemma 2.6)**.** *Consider two iterative sequences, each of r independent Bernoulli trials. Let $p_i, p'_i \in [0,1]$ denote the success probability of the i^{th} trial of the first and second sequence, respectively. Assume that $p_r = p'_r = 1$. For $i \in [r]$, let $q_i = p_i \cdot \prod_{j<i}(1-p_j)$ and $q'_i = p'_i \cdot \prod_{j<i}(1-p'_j)$. Let ε be such that for all $i \in [r]$, it holds that $\frac{p_i}{p'_i}, \frac{p'_i}{p_i}, \frac{(1-p'_i)}{(1-p_i)}, \frac{(1-p_i)}{(1-p'_i)} \in (1 \pm \varepsilon)$. Then, $\sum_{i=1}^{r-1} |q_i - q'_i| \leq 4\varepsilon(1-q_r)$.*

Proof. For every $j \in [r]$, let $\widetilde{p}_j = \min(p_j, p'_j)$, and for every $i \in [r]$ let $\widetilde{q}_i = \widetilde{p}_i \cdot \prod_{j<i}(1-\widetilde{p}_j)$. Since the $\widetilde{p}_j$s define an iterative sequence of Bernoulli trials, from Lemma A.3 and Lemma A.1 it follows

that,

$$\sum_{i=1}^{r-1} |q_i - q'_i| \leq \sum_{i=1}^{r-1} 3\varepsilon \cdot \widetilde{p}_j \cdot \left(\prod_{j<i}(1-\widetilde{p}_j)\right)\left(\frac{1}{3} + \sum_{j\leq i}\widetilde{p}_j\right) \tag{37}$$

$$\leq 3\varepsilon \cdot \sum_{i=1}^{r-1} \widetilde{q}_j \left(\frac{1}{3} + \sum_{j\leq i}\widetilde{p}_j\right) \tag{38}$$

$$= \varepsilon\left(\sum_{i=1}^{r-1}\widetilde{q}_j\right) + 3\varepsilon \cdot \left(\sum_{i=1}^{r}\widetilde{q}_j\left(\sum_{j\leq i}\widetilde{p}_j\right)\right) - 3\varepsilon\cdot\widetilde{q}_r\left(\sum_{j\leq r}\widetilde{p}_j\right) \tag{39}$$

$$\leq 4\varepsilon - 4\varepsilon\widetilde{q}_r \leq 4\varepsilon(1-q_r). \tag{40}$$

The second to last inequality uses the fact that $\widetilde{p}_r = p_r = p'_r = 1$. The last inequality follows since $1 - \widetilde{q}_r \leq 1 - q_r$. □

Proof of Fact 2.7. The first step of the induction is true since $C_1 = \mathbf{E}[D_1]$ is a constant and thus

$$\Pr\left[C_1 \geq \gamma \wedge \overline{D}_1\right] = \begin{cases} \mathbf{E}\left[\overline{D}_1\right] \leq 1-\gamma \leq e^{-\gamma} & \text{if } C_1 \geq \gamma \\ 0 \leq e^{-\gamma} & \text{if } C_1 < \gamma \end{cases}.$$

For the induction step,

$$\Pr\left[\sum_{i=1}^{r} C_i \geq \gamma \wedge \overline{D}_1 \wedge \ldots \wedge \overline{D}_r\right]$$

$$= \Pr\left[\overline{D}_1\right] \cdot \Pr\left[\sum_{i=2}^{r} C_i \geq \gamma - C_1 \wedge \overline{D}_2 \wedge \ldots \wedge \overline{D}_r \mid \overline{D}_1\right]$$

$$\leq (1-C_1) \cdot \max_{D_1(a_1)=0} \Pr\left[\sum_{i=2}^{r} C_i \geq \gamma - C_1 \wedge \overline{D}_2 \wedge \ldots \wedge \overline{D}_r \mid A_1 = a_1\right]$$

Notice that $A_1 = a_1$ induces a distribution on $A_2 \ldots A_r$ and that the hypotheses of the claim apply to the sequences $C_{i\geq 2}$ and $D_{i\geq 2}$. By induction hypothesis,

$$\Pr\left[\sum_{i=2}^{r} C_i \geq \gamma - C_1 \wedge \overline{D}_2 \wedge \ldots \wedge \overline{D}_r \mid A_1 = a_1\right] \leq e^{-\gamma + C_1}$$

and conclude that

$$\Pr\left[\sum_{i=1}^{r} C_i \geq \gamma \wedge \overline{D}_1 \wedge \ldots \wedge \overline{D}_r\right] \leq (1-C_1)\cdot e^{-\gamma+C_1} \leq e^{-\gamma}.$$

□

Proof of Fact 2.9. Straightforward computation.

$$\begin{aligned}
\mathbf{E}\left[A \mid B=b\right] &= \sum_a a \cdot \Pr\left[A=a \mid B=b\right] \\
&= \sum_a a \cdot \sum_c \Pr\left[A=a \wedge C=c \mid B=b\right] \\
&= \sum_a a \cdot \sum_c \Pr\left[A=a \mid B=b \wedge C=c\right] \cdot \Pr\left[C=c \mid B=b\right] \\
&= \sum_c \Pr\left[C=c \mid B=b\right] \cdot \sum_a a \cdot \Pr\left[A=a \mid B=b \wedge C=c\right] \\
&= \sum_c \Pr\left[C=c \mid B=b\right] \cdot \mathbf{E}\left[A \mid B=b, C=c\right] \in \pm\delta \ .
\end{aligned}$$

□

Proof of Fact 2.10. Straightforward computation. Fix $b' \in \mathrm{im}(f)$.

$$\begin{aligned}
&\mathbf{E}\left[\mathbf{E}\left[A \mid B\right] \mid f(B)=b'\right] \\
&\quad= \sum_b \mathbf{E}\left[A \mid B=b\right] \cdot \Pr\left[B=b \mid f(B)=b'\right] \\
&\quad= \sum_b \sum_a a \cdot \Pr\left[A=a \mid B=b\right] \cdot \Pr\left[B=b \mid f(B)=b'\right] \\
&\quad= \sum_b \sum_a a \cdot \Pr\left[A=a \wedge B=b \mid f(B)=b'\right] \\
&\quad= \sum_a a \cdot \Pr\left[A=a \mid f(B)=b'\right] = \mathbf{E}\left[A \mid f(B)=b'\right]
\end{aligned}$$

□

Proof of Fact 2.11. Straightforward computation. Fix $a' \in \mathrm{supp}(\mathbf{E}\left[A \mid B\right])$ and $b' \in \mathrm{im}(f)$.

$$\begin{aligned}
&\mathbf{E}\left[\mathbf{E}\left[A \mid B, C\right] \mid \mathbf{E}\left[A \mid B\right]=a', f(B)=b'\right] \\
&\quad= \sum_c \sum_{b\,:\,\substack{\mathbf{E}[A|B]=a' \\ f(B)=b'}} \mathbf{E}\left[A \mid B=b, C=c\right] \cdot \Pr\left[B=b \wedge C=c \mid \mathbf{E}\left[A \mid B\right]=a', f(B)=b'\right] \\
&\quad= \sum_c \sum_{b\,:\,\substack{\mathbf{E}[A|B]=a' \\ f(B)=b'}} \frac{\mathbf{E}\left[A \mid B=b, C=b\right] \cdot \Pr\left[B=b \wedge C=c\right]}{\Pr\left[\mathbf{E}\left[A \mid B\right]=a' \wedge f(B)=b'\right]} \\
&\quad= \sum_{b\,:\,\substack{\mathbf{E}[A|B]=a' \\ f(B)=b'}} \frac{\Pr\left[B=b\right]}{\Pr\left[\mathbf{E}\left[A \mid B\right]=a' \wedge f(B)=b'\right]} \cdot \sum_c \mathbf{E}\left[A \mid B=b, C=c\right] \cdot \Pr\left[C=c \mid B=b\right] \\
&\quad= a' \cdot \sum_{b\,:\,\substack{\mathbf{E}[A|B]=a' \\ f(B)=b'}} \frac{\Pr\left[B=b\right]}{\Pr\left[\mathbf{E}\left[A \mid B\right]=a' \wedge f(B)=b'\right]} \\
&\quad= a'
\end{aligned}$$

□

Proof of Fact 2.12. Let $B' = \mathsf{rnd}_\delta(B)$ and fix $b' \in [0,1]$ and $c \in \mathrm{supp}(C)$.

$$\begin{aligned}
\mathbf{E}\left[A \mid B' = b' \wedge C = c\right] &= \sum_a a \cdot \Pr\left[A = a \mid B' = b' \wedge C = c\right] \\
&= \sum_a a \cdot \sum_{b \in [b', b'+\delta]} \Pr\left[A = a \wedge B = b \mid B' = b' \wedge C = c\right] \\
&= \sum_a a \cdot \frac{1}{\Pr\left[B' = b' \mid C = c\right]} \sum_{b \in [b', b'+\delta]} \Pr\left[A = a \wedge B = b \mid C = c\right] \\
&= \frac{1}{\Pr\left[B' = b' \mid C = c\right]} \sum_{b \in [b', b'+\delta]} \Pr\left[B = b \mid C = c\right] \cdot \sum_a a \cdot \Pr\left[A = a \mid B = b \wedge C = c\right] \\
&= \frac{1}{\Pr\left[B' = b' \mid C = c\right]} \sum_{b \in [b', b'+\delta]} b \cdot \Pr\left[B = b \mid C = c\right] \\
&\in [b', b' + \delta]
\end{aligned}$$

□

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il