

On Aborts in Differential Privacy

Fredrik Meisingseth

Graz University of Technology, Austria
`fredrik.meisingseth@tugraz.at`

Abstract. There is a growing literature on differential privacy (DP) in multiparty protocols, enabling use in distributed settings and reduced trust assumptions. A largely overlooked aspect of such protocols is the extent to which an adversary can undermine the DP guarantees by making the protocol abort. Another is the DP properties of the honest parties' outputs. We initiate the study of both these issues.

First, we propose an idealized model of aborts, where an *aborter* is leaked some information about a DP mechanism execution and then chooses whether or not to let an independent malicious analyst learn the mechanism output. We bound the effects of aborts according to what information (the database, randomness, output, or any combination of these) is leaked. These bounds are not only applicable to multiparty DP via general-purpose multiparty computation (MPC) but may also be used in the analysis of other methods to certify DP properties of a protocol. Second, we apply these bounds to analyze ideal protocol executions in MPC. We show, for the first time, that the ideal execution with fairness gives strictly stronger DP guarantees than that for security-with-abort, for the outputs to the honest parties. Further, solitary-output functionalities satisfy guarantees similar to those of the execution with fairness. Finally, we analyze multiparty protocols with respect to the way in which they realize the respective ideal functionalities. We show that partially fair and fully fair protocols have very similar DP guarantees. Since partial fairness, as opposed to full fairness, can be achieved in dishonest-majority settings, and in particular the two-party setting, this opens up for enhanced DP guarantees in two-party computation.

1 Introduction

In the central ('curator') model of differential privacy (DP) [21,19], one must trust the curator to execute the supposed DP mechanism faithfully. This may be problematic, for instance if the curator is a company with vested interest in the outcome of the computation because it is indicative of the performance of the company. One approach for reducing the need to trust a curator is to replace it with a multiparty computation (MPC) protocol. Such *multiparty DP* protocols have gathered much attention, in both theoretical [6,45,40,33,32,34] and applied [20,14,52,42,38,23] works.

So far in multiparty DP, the mapping within the protocol which is required to be DP is that from the honest parties' inputs to the view of the adversary [6,45,42]. This is a reasonable goal when each party holds a partial dataset

in the clear, and one is not concerned with protecting the inputs from corrupted parties, and when the outputs to the honest parties are never given to any potentially malicious analyst. We argue that the DP guarantees of the outputs to the honest parties are, in many cases, crucial, and that these may be important even w.r.t. the inputs of the malicious parties. Consider again a malicious company which claims to publish DP statistics about its customers. Some external honest party (say, a data protection agency) runs a multiparty DP protocol with the company (contributing no data) and then releases the result publicly on behalf of the company. Now, the DP guarantees of interest should be those of the mapping from the users' data (i.e. input of the corrupted party) to the public output (i.e. output to the honest party). Another example is a group of researchers, each with a sensitive dataset, where one (honest) party is designated as the one which will report the results from this joint study to the public. We note that the adversary's view being DP with respect to the inputs of the honest parties is not known to imply that the outputs to the honest parties are DP, neither with respect to the inputs of the honest parties nor those of the corrupted ones.

Furthermore, one commonly uses *security-with-abort* (SwA) [53,26,28] as the notion of secure computation in multiparty DP, either for efficiency or because it is necessary within one's MPC setting. SwA means that an adversary cannot change the outcome of the protocol arbitrarily, but they can receive their output and thereafter make the protocol abort, thereby preventing the honest parties from getting an output. For probabilistic computations, as with DP mechanisms, such selective aborts may distort the distribution of the output, even when only considering the protocol executions that do not abort.

We therefore study the effects of aborts in multiparty DP protocols, not only on the view of the adversary but also on the outputs to the honest parties (or some dedicated output-party), with respect to either the entire used database (including the inputs of malicious parties) or only the inputs of honest parties. We refer to these outputs as the *public output* of the protocol. We further study the effects of aborts on the public output conditioned on it not being an abort. This is important, as that is the output distribution arising in the case that the protocol is simply re-run until it gives a non-aborting public output. To our knowledge, we are the first to study either of these aspects of multiparty DP. One specific natural question left open in previous work is:

Do multiparty DP protocols with fairness give stronger privacy guarantees than multiparty DP protocols that are secure-with-abort?

We resolve this question in the positive – fairness is a strict improvement upon SwA when considering the public output, especially with respect to the inputs of the honest parties. We also show that *partial fairness* [29,30] results in similar DP and accuracy guarantees to full fairness.

Summary of contributions.

1. We propose an idealized model for studying the effects of selective aborts in DP protocols (Section 3), on both the output distribution directly and the

distribution when conditioned on it not being an abort. We give (Section 4) upper and lower bounds (see Table 1) on the generally achievable DP parameters dependent on the information available to the aborter, as a function of the maximal abort probability and the DP guarantees of the intended target mechanism.

2. We apply these bounds to ideal protocol executions for MPC protocols computing DP mechanisms and bound the DP and accuracy guarantees (Section 5). This includes the first analyses in multiparty DP of the DP properties of the honest parties' outputs, the difference in guarantees with respect to the inputs of the honest parties and those of the corrupted ones, and of solitary-output functionalities. The main take-away is that fairness does give strictly stronger DP and accuracy guarantees than security-with-abort.
3. We apply these results to derive bounds on the DP and accuracy properties of protocols emulating said ideal protocol executions under different notions of secure computation, including statistical/computational security and partial fairness (Section 6). The main take-away is that partial fairness gives only slightly weaker guarantees than full fairness.

1.1 Technical Overview

We restrict our attention to additive-noise mechanisms, i.e. those $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ of the form $\mathcal{M}(\cdot) := f(\cdot) + Z$, for a function $f : \mathcal{D} \rightarrow \mathcal{R}$ and a noise distribution Z over $\mathcal{R}$. We specify DP guarantees in terms of privacy profiles [4] and accuracy in terms of (α, β) -accuracy (Definition 2).

The idealized model of aborts. Towards the goal of understanding the DP and accuracy guarantees of multiparty DP protocols, we introduce an model of aborts (MoA).¹ A malicious party A , called the *aborter*, is given leakage about an execution of an $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP mechanism $\mathcal{M}$ execution must then choose whether a separate malicious analyst² should be given the mechanism output or not. We analyze the effects of aborts according to the information available to the aborter, being some subset of the database, noise sample, and outcome. This information is described by a *leakage type* $\text{leak} \subseteq \{\text{DB}, \text{sample}, \text{outcome}\}$. We give concrete upper and lower bounds on the DP parameters, given that one assumes an upper bound $\gamma_{\perp}$ on the abort probability. These bounds are for the parameters that can be guaranteed for *every* additive-noise $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP target mechanism and all choices of $\gamma_{\perp}$ and ε . That is, we treat $\mathcal{M}$ in a black-box manner, and the bounds on the privacy profile of $\mathcal{M}'$ are relative to the profile

¹ The benefit of using this model is that it lets us isolate the effects of abort from other potential adversarial effects within a protocol. This motivation is akin to that of the fail-stop model of Cleve and Impagliazzo [16], used for studying the effects of aborts in coin-tossing protocols.

² This analyst is the traditional adversary in DP.

of $\mathcal{M}$. Therefore, a lower bound means that there exists some tuple $(\mathcal{M}, \varepsilon, \gamma_\perp)$ for which the DP parameters cannot be strictly lower.³

Let $\mathcal{M}'_A$ be the mechanism with aborts described above, for a specific aborter A , and let $\mathcal{M}'_{A \neq \perp}$ be $\mathcal{M}'_A$ conditioned on it not aborting. To see that the information available to the aborter A will make a large difference, consider these two extreme scenarios:

1. A always chooses to abort, regardless of the database, noise sample or outcome. Then $\mathcal{M}'_A$ is $(0, 0)$ -DP, as its output is independent of the database.
2. A selects one database D and always aborts if that database is used. For every other database D' , A never aborts. Then, $\mathcal{M}'_A$ aborting is a perfect indicator that the input was D , so $\mathcal{M}'$ provides no better than $(0, 1)$ -DP (i.e. no privacy at all).

If $\mathcal{M}$ has reasonable parameters $(\varepsilon > 0, \delta < 1)$, then $\mathcal{M}'$ has stronger privacy guarantees than $\mathcal{M}$ in the first example, but weaker in the second. So depending on the strategy of the aborter, and the information available, the privacy guarantees may either be improved or worsened by the existence of an aborter. As tools for deriving the later bounds, we establish a number of useful facts about the model. The core ones are, informally:

- If $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP then $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_\perp)$ -DP and if $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP then $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$ -DP (Lemma 1).
- If the view of the aborter can be simulated from only a subset of the leakage it gets then the DP and accuracy guarantees of $\mathcal{M}'$ with respect to A will be no worse than those when the aborter is given only this subset of information (Lemma 2).
- The DP and accuracy parameters of $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$ cannot improve by giving the aborter more information (Lemma 3). We call this the *hierarchy lemma*.
- The DP and accuracy parameters of $\mathcal{M}'$ for $\text{leak} = \{\text{DB}, \text{sample}\}$, $\text{leak}' = \{\text{DB}, \text{outcome}\}$ and $\text{leak}'' = \{\text{DB}, \text{sample}, \text{outcome}\}$ are identical (Lemma 4).

These results lead straight-forwardly to general (leakage type independent) upper and lower bounds (Theorem 2): For every leakage type, $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$ -DP, and their parameters are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$. This is, however, often far from optimal.

Deriving better bounds. Some of the leakage types exhibit a structure which enables us to show improved bounds for that leakage type specifically. For others, we can often use the technical lemmas listed above to extend results from one type to another, or to extend bounds between $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$.

For the simplest case of $\text{leak} = \{\}$, we observe that the output distribution of $\mathcal{M}'_A$ is equivalent to that arising if one simply runs $\mathcal{M}'_{A \neq \perp}$ with some fixed probability and otherwise runs another mechanism $\bar{\mathcal{M}}$ which always aborts. That is, $\mathcal{M}'$ is a *mixture mechanisms* [50,4] between $\mathcal{M}'_{A \neq \perp}$ and $\bar{\mathcal{M}}$. By the definition

³ It may be possible to find stronger bounds for specific mechanisms. We leave for future work to explore mechanism-specific bounds.

of $\mathcal{M}'_{A \neq \perp}$, it can be shown to be $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP (Theorem 1), and $\bar{\mathcal{M}}$ clearly is $(0, 0)$ -DP. As, roughly, the parameters for mixture mechanisms are the averages of the parameters for the constituent mechanisms, we learn that for $\text{leak} = \{\}$, an increased abort probability always leads to improved DP parameters. Thus, for every upper bound $\gamma_{\perp}$ on the abort probability, the aborter which gives the worst DP parameters is the one which never aborts. Hence $\mathcal{M}'$ for $\text{leak} = \{\}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP (Theorem 3).

For $\text{leak} = \{\text{sample}\}$, we can again formulate $\mathcal{M}'$ as a mixture mechanism, since the abort probability is independent of the database. However, we have no bound showing that $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and therefore, we use the generic upper bound of $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^{\varepsilon} + 1)\gamma_{\perp})$ -DP. This leads to parameters for $\mathcal{M}'$ being strictly better than the general bound, although for some $\mathcal{M}$ and choices of $\varepsilon, \gamma_{\perp}$ it is above $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ (Theorem 4).⁴

For $\text{leak} = \{\text{outcome}\}$, we can no longer phrase $\mathcal{M}'$ as a mixture model, since the abort probability is dependent of the database. We can, however, use preservation under post-processing [22,49], since the aborter simply post-processes mechanism output, to derive that $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. This in turn implies that $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_{\perp})$ -DP (by Lemma 1). We then show our first improved lower bound, for $\mathcal{M}'_{\neq \perp}$. We do this by constructing an aborter for a fixed target mechanism $\mathcal{M}$ (the geometric mechanism [25]) and deriving its exact privacy parameters (Theorem 5). By choosing suitable parameters $\varepsilon, \gamma_{\perp}$, we show that there is a value $c_{\mathcal{M}} \in (0, 1)$ such that the parameters for $\mathcal{M}'_{\neq \perp}$ are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}} \cdot \gamma_{\perp})$.

For $\text{leak} = \{\text{DB}\}$, $\mathcal{M}'_{\neq \perp}$ is again $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and Lemma 1 then implies that $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon}\gamma_{\perp})$ -DP. We show that this is tight by translating a corresponding lower bound from the literature on certifiable DP [7]. This lower bound also applies to the remaining leakage types, by the hierarchy lemma. Similarly, the lower bound for $\mathcal{M}'_{\neq \perp}$ from the case of $\text{leak} = \{\text{outcome}\}$ also extends to the remaining leakage types.

Table 1 summarizes the upper and lower bounds on the generally achievable DP parameters in the MoA.

Applying the bounds to ideal protocol executions. The bounds from the MoA can be used to derive the DP guarantees of the ideal protocol executions of DP mechanisms, with SwA and fairness, respectively. For these results, we use the standard standalone formulation of the ideal protocol executions [12,27]. We additionally analyze the special two-party case of *solitary-output functionalities* (SOFs) [35,3], where a *sender* holds the entire input and a *receiver* is the only one getting an output. We restrict our attention to functionalities where all parties that get output get the same output. We analyze the guarantees of the output with respect to either only the inputs of the honest parties, denoted D_H , or with respect to the entire used database $\bar{D}$. Since the adversary can choose the inputs from the corrupted parties freely, this used database $\bar{D}$ consists of D_H

⁴ As we do not have a clean closed form for this bound, we do not include it in the introduction.

Table 1. Bounds on the privacy profiles in the MoA for the respective leakage types, given that the probability of abort (for every database) is at most $\gamma_\perp$. $c_{\mathcal{M}} \in (0, 1)$ is a mechanism-specific constant. ‘S’ denotes ‘sample’ and ‘O’ denotes ‘Outcome’. The fifth column describes the characteristics of the bounds. For upper bounds, $\bigcirc$ = ‘generic bound’, $\bullet$ = ‘lower than generic bound, but monotone increasing in $\gamma_\perp$ ’, and $\bullet$ = ‘optimal’. For lower bounds, $\bigcirc$ = ‘above $\delta_{\mathcal{M}}(\varepsilon)$ ’ and $\bullet$ = ‘exactly $\delta_{\mathcal{M}}(\varepsilon)$ ’.

leak	Mech.	Upper bound	Lower bound	Char.	Theorems
DB,S,O	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
DB,O	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
DB,S	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp$	$\bigcirc/\bigcirc$	2, 7
DB	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\bullet/\bigcirc$	6, Lemma 10
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon)$	$\delta_{\mathcal{M}}(\varepsilon)$	$\bullet/\bullet$	1, 2
S,O	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$	$\bigcirc/\bigcirc$	2, 8
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp$	$\bigcirc/\bigcirc$	2, 8
O	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon)$	$\delta_{\mathcal{M}}(\varepsilon)$	$\bullet/\bullet$	2, 5
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + \gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp$	$\bullet/\bigcirc$	5
S	$\mathcal{M}'$	See Thm. 4	$\delta_{\mathcal{M}}(\varepsilon)$	$\bullet/\bullet$	2, 4
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp$	$\delta_{\mathcal{M}}(\varepsilon)$	$\bigcirc/\bullet$	2, 4
None	$\mathcal{M}'$	$\delta_{\mathcal{M}}(\varepsilon)$	$\delta_{\mathcal{M}}(\varepsilon)$	$\bullet/\bullet$	2, 3
	$\mathcal{M}'_{\neq \perp}$	$\delta_{\mathcal{M}}(\varepsilon)$	$\delta_{\mathcal{M}}(\varepsilon)$	$\bullet/\bullet$	1, 2

Table 2. DP and accuracy results for the public output Out^S in the ideal protocol executions for SwA, fairness and SOFs, under the assumption that $\mathcal{S}$ aborts with probability at most $\gamma_\perp$. SOF_s and SOF_r denote the cases that the sender and receiver is corrupted, respectively. * In SOF when the sender is corrupted, there is no D_H .

Model	Mech.	Acc. w.r.t. $\bar{D}$	DP w.r.t. D_H	DP w.r.t. $\bar{D}$
SwA	Out^S	$(\alpha, \beta + \gamma_\perp)$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$
	$\text{Out}^S_{\neq \perp}$	$(\alpha, \beta + \gamma_\perp)$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_\perp)$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$
Fair	Out^S	$(\alpha, \beta + \gamma_\perp)$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$
	$\text{Out}^S_{\neq \perp}$	(α, β)	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$
SOF_s	Out^S	$(\alpha, \beta + \gamma_\perp)$	-*	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$
	$\text{Out}^S_{\neq \perp}$	(α, β)	-*	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$
SOF_r	Out^S	$(\alpha, \beta + \gamma_\perp)$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$
	$\text{Out}^S_{\neq \perp}$	(α, β)	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$	$(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$

and the chosen inputs $\bar{D}_C$ from the corrupted ones. For an ideal-world adversary $\mathcal{S}$, let $\text{Out}^{\mathcal{S}}(\bar{D})$ denote the distribution of the public output.

A summary of the results for ideal executions is found in Table 2. In every case except for SOFs with corrupted sender, the view of the adversary has the same guarantees as $\text{Out}^{\mathcal{S}}$, w.r.t. D_H . These results are all proven by relating each $\mathcal{S}$ to some corresponding aborter in the MoA (Lemmas 12 to 15), and then applying the previously derived bounds. Consider, for example, the ideal execution for SwA and the DP guarantees of $\text{Out}^{\mathcal{S}}$ with respect to D_H . The adversary $\mathcal{S}$ has only three ways of affecting $\text{Out}^{\mathcal{S}}$; It can choose the inputs from the corrupted parties, it can abort before having gotten an output, and it can abort after having gotten an output. The choice of inputs will not have an impact on the DP guarantees of $\text{Out}^{\mathcal{S}}$ (Lemma 11), essentially because it would contradict the fact that the target mechanism $\mathcal{M}$ is DP. This means that $\mathcal{S}$ can only influence the DP properties of $\text{Out}^{\mathcal{S}}$ by aborting, and the only information available to it when choosing whether or not to abort is the outcome of $\text{Out}^{\mathcal{S}}$. Hence, intuitively, the DP and accuracy guarantees of the public output w.r.t. the inputs of the honest parties, for SwA, should be equivalent to $\mathcal{M}'$ in the MoA for the case $\text{leak} = \{\text{outcome}\}$. This line of reasoning applies to all of the considered ideal executions. Therefore, we can show that fairness leads to stronger DP guarantees than SwA by showing that fairness corresponds to the MoA for a smaller leakage type (Theorems 9 to 11).

Analyzing multiparty protocols. Having proven the guarantees of ideal executions of DP mechanisms, we can analyze the guarantees of protocols according to the way in which they emulate such an ideal execution. Securely realizing a functionality means that there is a bound on the distances between the adversarial views and the public outputs between real and ideal protocol executions. As we have already proven bounds on the DP and accuracy parameters in the ideal protocol executions, we only need to analyze how the distance between the ideal and real worlds affect those parameters. For standard statistical or computational security, this is rather straight-forward as the protocol essentially inherits the properties of the ideal execution, and the parameters are increased by at most a negligible amount. For partially fair protocols [29], the closeness guarantee is that the ideal and real worlds have a computational distance of at most $1/p$, for some polynomial p . By utilizing a hybrid indistinguishability lemma [10,43], we can show that such a bound on computational distance implies that the real public output is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)/p)$ -IND-CDP (computationally DP [45]) whenever the ideal public output is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP.

1.2 Practical Discussion

Our results have several implications for the design of multiparty DP protocols in practice, apart from showing that fairness is preferable to SwA.

Firstly, there is the clear structure that giving the adversary more information allows their abort-decision to have a much larger impact on the final DP parameters. This means that one should, if feasible for one's use-case, minimize

the information available to any potential adversary. This can, for instance, be done by having the users/clients secret-share their data between computational parties, as done in Prio [17,37,2], instead of letting each computational party hold part of the database in the clear.

Secondly, for some leakage types there is a large difference between the DP parameters of $\mathcal{M}'$ and those of $\mathcal{M}'_{\neq \perp}$. This means that honest parties should be mindful about publicly revealing whether or not the protocol has been aborted, even if they eventually receive a non-aborting output. It also means that one, in analyzing a DP system where selective aborts may occur, should be careful of arguing that all non-aborting protocol executions give the same DP guarantees as the target mechanism, as this is not always the case.

Thirdly, one may in practice be able to encourage the adversary to not abort, by using protocols that allows one to identify the aborter and levy a penalty on parties that abort [8]. Our results show that for some leakage types, doing so has no effect on the final DP guarantees, as those are independent of the abort probability. For other leakage types, the increase in δ is linear in the maximal abort probability, meaning that one in that case should make the penalty heavy enough to make the (likely) maximal abort probability not much larger than $\delta_{\mathcal{M}}(\varepsilon)$. Otherwise the final δ -parameter will potentially be dominated by the effects of aborts. For example, say that $\mathcal{M}$ is the geometric mechanism [25] parameterized such that $\mathcal{M}$ is $(\varepsilon, 0)$ -DP for $\varepsilon = \ln(2)$, let the adversary/aborter in the protocol have access to the database, and let the penalty be such that $\Gamma_{\perp}^{\max}(\mathcal{M}, A) \leq 1/100$ with high probability. Then, by the lower bound for $\text{leak} = \{\text{DB}\}$, the DP properties of the public output cannot be better than $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon} \Gamma_{\perp}^{\max}(\mathcal{M}, A)) = (\varepsilon, 0 + 2 \cdot 1/100) = (\varepsilon, 2/100)$. In many cases, there is a fundamental qualitative difference between $(\varepsilon, 0)$ -DP and $(\varepsilon, 2/100)$ -DP.

1.3 Related Works

Aborts are not an issue in the central model of DP as the curator is assumed to be honest. In multiparty DP, the earliest works considered either passive adversaries that follow the protocol and thus do not abort [6], or assume that less than one third of the parties are corrupted and thus fairness can be achieved [20]. The first work treating adversaries that may abort [45], shows that SwA suffices for the view of the adversary to be computationally DP with respect to the inputs from the honest parties, regardless of the abort probability. The study of multiparty DP has since, to the best of our knowledge, remained within these settings where aborts are not an issue, either because they are assumed not to occur or because one only considers the adversary's view.

An alternative to multiparty DP is *certifiable/verifiable DP* [9,7,48,44,47,1], where the curator essentially uses an interactive proof (with the analyst) to prove that they have executed the target mechanism faithfully. It has been shown, roughly, that the curator (having access to the database, noise sample and outcome) can increase the final δ -parameter at most proportionally to the probability that they cause an abort [7]. There are, however, no works analyzing what information the curator must have in order to cause such an increase, nor the

guarantees that the output fulfills when conditioning on it not being an abort. There is also no work formally comparing the differences in security, privacy and accuracy properties between certifiable DP and multiparty DP. Therefore, we believe that our model of aborts will also be useful within the context of certifiable DP. For instance, our results indicate (see Table 1) that the curator cannot, in general, be prevented from increasing the DP parameters if they have access to the noise sample or database.

1.4 Open Directions

One immediate open direction is to close the gaps between our upper and lower bounds. Gaps of particular interest are those where the upper bound is worse than $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP but the lower bound is the general one of precisely $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP, such as for $\text{leak} = \{\text{sample}\}$. This translates to the question if aborts based solely on knowledge of the noise sample do indeed lead to worse DP parameters compared to the target mechanism, either in general or for some specific target.

Another open direction is to study mechanism-specific upper and lower bounds for, say, the discrete Gaussian mechanism [13]. Our upper bounds apply, but not all our lower necessarily do. It is therefore a possibility that this mechanism, or some other important one, leads to significantly better DP guarantees in the presence of aborts than our mechanism-independent upper bounds imply.

Finally, our bounds open up for a formal comparison of the security, privacy and accuracy guarantees between concrete protocols in the space of multiparty DP and certifiable DP. As outlined in the practical discussion above, the results also suggest ways of potentially improving existing protocol constructions by either changing the information available to any potential adversary or by dictating whether or not it should be disclosed when a protocol is aborted.

2 Preliminaries and Notation

An arbitrary negligible function is denoted negl and κ is the security parameter. We denote the computational distance between two distribution ensembles X, Y by $CD(X, Y)$ and the statistical (total variation) distance by $SD(X, Y)$. If the distance is upper bounded by a function $\eta(\kappa)$, we write $X \approx_{\eta}^c Y$ (i.e., they are computationally η -distinguishable [29]) and $X \approx_{\eta}^s Y$, respectively. We denote X and Y being identically distributed by $X \sim Y$.

2.1 Differential Privacy

Definition 1 ([21,19]). Let $\varepsilon \geq 0, \delta \in [0, 1]$ and $\mathcal{D}, \mathcal{R}$ be discrete sets. A probabilistic algorithm $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ is (ε, δ) -differentially private (DP) if for all adjacent $D, D' \in \mathcal{D}$ (i.e. that differ in at most one element) in $\mathcal{D}$ and all $S \subseteq \mathcal{R}$,

$$\mathbb{P}(\mathcal{M}(D) \in S) \leq e^{\varepsilon} \mathbb{P}(\mathcal{M}(D') \in S) + \delta.$$

We let $\mathcal{D}$ and $\mathcal{R}$ be arbitrary, but require that $\mathcal{R}$ has an associated norm. In our application to MPC, we require that $\mathcal{M}$ is polynomial-time computable.

Definition 2. Let $\alpha \geq 0, \beta \in [0, 1]$ and define $|\perp - s| = \infty$ for all $s \in \mathcal{R}$. A mechanism $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R} \cup \{\perp\}$ is called (α, β) -accurate for query $f : \mathcal{D} \rightarrow \mathcal{R}$ if for every $D \in \mathcal{D}$: $\mathbb{P}(|\mathcal{M}(D) - f(D)| > \alpha) \leq \beta$.

Every mechanism $\mathcal{M}$ fulfills an infinite set of (ε, δ) pairs, and all these (optimal) pairs can be described by phrasing δ as a function of ε . This mechanism-specific function $\delta_{\mathcal{M}}(\cdot)$ is called the *privacy profile* of $\mathcal{M}$ [4].

In an MPC protocol, it is often impossible to achieve (statistical) DP, as the protocol only satisfies computational security. Therefore, it is necessary to relax to *computational DP* (CDP), which can be done in different natural ways.

Definition 3 ([45,42]). An ensemble $\mathcal{M}'$ of mechanisms $\mathcal{M}'_{\kappa} : \mathcal{D}_{\kappa} \rightarrow \mathcal{R}_{\kappa}$ is (ε, δ) -SIM-CDP if there exists a negligible function negl and an ensemble $\hat{\mathcal{M}} = \{\hat{\mathcal{M}}_{\kappa}(\cdot) : \mathcal{D}_{\kappa} \rightarrow \mathcal{R}_{\kappa}\}_{\kappa \in \mathbb{N}}$ of (ε, δ) -DP mechanisms such that for all polynomial-size inputs D , we have $\mathcal{M}'(D) \approx_{\text{negl}(\kappa)}^c \hat{\mathcal{M}}(D)$.

Definition 4 ([6,45]). A mechanism ensemble $\mathcal{M}'$ is (ε, δ) -IND-CDP if there exists a negligible function negl such that for every polynomial-time computable predicate T , every sufficiently large κ and all polynomial-sized adjacent $D, D' \in \mathcal{D}_{\kappa}$, we have $\mathbb{P}(T(\mathcal{M}'_{\kappa}(D)) = 1) \leq e^{\varepsilon \kappa} \mathbb{P}(T(\mathcal{M}'_{\kappa}(D')) = 1) + \delta_{\kappa} + \text{negl}(\kappa)$.

The CDP definitions treat *ensembles* of mechanisms, and this is necessary because the mapping within a protocol which is analyzed (like that from the honest parties' inputs to the adversarial view) is dependent on the security parameter, even if the target mechanism is the same for all κ . For simplicity, we later ignore the difference between a mechanism and an ensemble, and omit the security parameter from notation.

There is a rich literature on the relationship between the different flavors of CDP and statistical DP [45,31,11,41,24,42,43]. For our work, the only needed background is that (ε, δ) -SIM-CDP implies (ε, δ) -IND-CDP if ε is at most logarithmic (we assume that ε is constant), but that there is no known 'natural' [49] computational task computable with IND-CDP but not SIM-CDP. However, since SIM-CDP is stronger, we use it primarily but do rely on IND-CDP in one lemma (Section 6.2) which is not known to hold for SIM-CDP.

2.2 Secure Multiparty Computation

We work in the standalone model of secure multiparty computation. For a full description of the model, see [27,39,12]. We consider only static corruptions from active adversaries. An n -party functionality $\mathcal{F}_{\mathcal{M}}$ is a sequence of polynomial-time computable randomized mappings $\{\mathcal{M}_{\kappa} : \chi^n \rightarrow \mathcal{R}^n\}$. We restrict our attention to functionalities which take inputs from the same domain for all parties and where the outputs given to each party are either identical or $\perp$ (denoting abort).

To align with the notation for DP mechanisms, we let every $\mathcal{M}_\kappa$ be identical, and simply denote it $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$.

Security is defined by statistical or computational closeness between an ideal world, which is secure by definition, and the real world. The ideal world consists of a trusted and incorruptible party computing $\mathcal{F}_\mathcal{M}$, dummy parties that simply send their input to the trusted party and receive outputs, and an ideal-world adversary/simulator $\mathcal{S}$ which interacts only with $\mathcal{F}_\mathcal{M}$. The interactions in the ideal world follows a prescribed ideal protocol execution, versions of which we recall in Section 5. The execution in the real world is simply the execution of the protocol Π , with an adversary $\mathcal{A}$ corrupting some parties in a way corresponding to a given $\mathcal{S}$. Let $\text{Ideal}_{\mathcal{F}_\mathcal{M}, \mathcal{S}}(D_1, \dots, D_n, \kappa)$ be the joint distribution of the view of the adversary $\mathcal{S}$ and the outputs to the honest parties, within the ideal execution with inputs $D_1, \dots, D_n$ for security parameter κ . Similarly, $\text{Real}_{\Pi, \mathcal{A}}(D_1, \dots, D_n, \kappa)$ is the corresponding distribution in a real execution of the protocol Π . A protocol Π securely realizes $\mathcal{F}$ with computational security if for every PPT $\mathcal{A}$ there exists an PPT $\mathcal{S}$ such that for every set of inputs $D_1, \dots, D_n$: $\text{Ideal}_{\mathcal{F}_\mathcal{M}, \mathcal{S}}(D_1, \dots, D_n, \kappa) \approx_{\text{negl}}^c \text{Real}_{\Pi, \mathcal{A}}(D_1, \dots, D_n, \kappa)$. If the same holds also for unbounded adversaries, and with statistical indistinguishability, then Π achieves statistical security.

3 The Idealized Model of Aborts (MoA)

We give an idealized model of aborts (MoA) for DP mechanisms. We model an aborter strategy as a probabilistic algorithm A from some view to one of $\top$ (denoting ‘continue’) and $\perp$ (denoting ‘abort’). The view is represented as the output of a probabilistic function which is given a leakage vector L as input. This leakage vector contains a subset of the database D , the noise sample z and the outcome (mechanism output) s .

Definition 5 (Aborting mechanism). *Let $f : \mathcal{D} \rightarrow \mathcal{R}$ be a function, Z be a distribution over $\mathcal{R}$ and let $\mathcal{M}(\cdot) := f(\cdot) + Z$. Let $\text{leak} \subseteq \{\text{DB}, \text{sample}, \text{outcome}\}$ and VIEW be a probabilistic function between $(\mathcal{D} \cup \{\top\}) \times (\mathcal{R} \cup \{\top\}) \times (\mathcal{R} \cup \{\top\})$ and $\{0, 1\}^*$. Let A be a probabilistic algorithm $\{0, 1\}^* \rightarrow \{\perp, \top\}$. Define $\mathcal{M}'_A : \mathcal{D} \rightarrow \mathcal{R} \cup \{\perp\}$ for $(\mathcal{M}, \text{leak}, \text{VIEW})$ as follows:*

1. **Compute:** Sample $z \leftarrow Z$ and set $s = f(D) + z$.
2. **Leak:** If $\text{DB} \in \text{leak}$, set $L_1 = D$ and otherwise set $L_1 = \top$. If $\text{sample} \in \text{leak}$, set $L_2 = z$ and otherwise set $L_2 = \top$. If $\text{outcome} \in \text{leak}$, set $L_3 = s$ and otherwise set $L_3 = \top$. Set $L = (L_1, L_2, L_3)$.
3. **Abort:** If $A(\text{VIEW}(L)) = \perp$ then output $\perp$, otherwise output s .

We call $\mathcal{M}$ the target mechanism, and assume throughout that it is $(\epsilon, \delta_\mathcal{M}(\epsilon))$ -DP and (α, β) -accurate. We call leak the leakage type and A the aborter strategy, or simply *aborter*.

Definition 6. *For $D \in \mathcal{D}$, $\mathcal{M}$, leak and A , the total probability of abort is denoted $\Gamma_\perp(D, \mathcal{M}, A) := \mathbb{P}(\mathcal{M}'_A(D) = \perp)$. The maximal abort probability of $\mathcal{M}'_A$ over all databases is denoted $\Gamma_\perp^{\max}(\mathcal{M}, A) := \max_{D \in \mathcal{D}} \{\Gamma_\perp(D, \mathcal{M}, A)\}$.*

The abort probability $\Gamma_\perp$ is necessarily a function of $D, \mathcal{M}$ and A , dependent on leak. We typically omit these dependencies from notation, but include them when necessary for clarity. Let $\mathbf{Ab}$ denote the set of all probabilistic functions from $\{0, 1\}^*$ to $\{\top, \perp\}$ and define $\mathcal{M}'$ as the set $\{\mathcal{M}'_A : A \in \mathbf{Ab}\}$.

Definition 7. Let $\delta_{\mathcal{M}'} : [0, \infty) \times [0, 1] \rightarrow [0, 1]$. $\mathcal{M}'$ is called $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP for $(\mathcal{M}, \text{leak}, \text{VIEW})$ if $\mathcal{M}'_A$ for $(\mathcal{M}, \text{leak}, \text{VIEW})$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP for every $\varepsilon, \gamma_\perp \geq 0$ and every aborter strategy $A \in \mathbf{Ab}$ with $\Gamma_\perp^{\max}(\mathcal{M}, A) \leq \gamma_\perp$.

Let $\delta'_{\mathcal{M}'} : [0, \infty) \times [0, 1] \rightarrow [0, 1]$. We say that the DP parameters of $\mathcal{M}'$ for $(\mathcal{M}, \text{leak}, \text{VIEW})$ are lower-bounded by $(\varepsilon, \delta'_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ if there exists some tuple $(\varepsilon, \gamma_\perp, A)$ as above such that $\mathcal{M}'_A$ is not (ε, δ') -DP for any value $\delta' < \delta'_{\mathcal{M}'}(\varepsilon, \gamma_\perp)$.

We define the accuracy of $\mathcal{M}'$ analogously. We ask ourselves what DP and accuracy guarantees $\mathcal{M}'$ fulfills given a choice of $\mathcal{M}, \text{leak}, \text{VIEW}$ and $\gamma_\perp$.

3.1 Conditioning On Not Aborting

We consider the guarantees of non-aborting outcomes under the different leakage types. Operationally, this can be quite satisfactory, since it means that *either* there is an abort *or* the output satisfies known DP and accuracy guarantees. Let $\mathcal{M}'_{A \neq \perp}$ denote $\mathcal{M}'_A$ conditioned on it not outputting $\perp$. That is, for all $S \subseteq \mathcal{R}$ and $D \in \mathcal{D}$,

$$\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) \in S) := \frac{\mathbb{P}(\mathcal{M}'_A(D) \in S)}{1 - \Gamma_\perp(\mathcal{M}, D, A)},$$

if $\Gamma_\perp^{\max}(\mathcal{M}, A) < 1$. If $\Gamma_\perp^{\max}(\mathcal{M}, A) = 1$ then $\mathcal{M}'_{A \neq \perp}$ is ill-defined, so in all statements about $\mathcal{M}'_{A \neq \perp}$, we assume that $\Gamma_\perp^{\max}(\mathcal{M}, A) < 1$. Define $\mathcal{M}'_{\neq \perp} := \{\mathcal{M}'_{A \neq \perp} : A \in \mathbf{Ab}\}$ and $\mathcal{M}'_{\neq \perp}$ being DP, and accurate, analogously to how we define it for $\mathcal{M}'$.

Lemma 1. *The following holds for all $\mathcal{M}, \text{leak}, A, \text{VIEW}$:*

- $\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) \in S) \geq \mathbb{P}(\mathcal{M}'_A(D) \in S)$ for all $S \subseteq \mathcal{R}, D \in \mathcal{D}$.
- $\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) \in S) \leq \mathbb{P}(\mathcal{M}'_A(D) \in S) + \Gamma_\perp(\mathcal{M}, D, A)$ for all $S \subseteq \mathcal{R}, D \in \mathcal{D}$.
- If $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP then $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + \gamma_\perp)$ -DP.
- If $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP then $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + e^\varepsilon \gamma_\perp)$ -DP.

Proof. The first two bullet-points follow directly from the definition of $\mathcal{M}'_{A \neq \perp}$, since $\Gamma_\perp(\mathcal{M}, A) \in [0, 1]$. Now assume that $\Gamma_\perp(\mathcal{M}, D, A) \leq \gamma_\perp$ for all D and some $\gamma_\perp \in [0, 1]$. For the third point, we have for every $\mathcal{M}, \text{leak}, A, \text{VIEW}, S \subseteq \mathcal{R}$ and all adjacent $D, D' \in \mathcal{D}$ that

$$\begin{aligned} \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) \in S) &\leq \mathbb{P}(\mathcal{M}'_A(D) \in S) + \Gamma_\perp(\mathcal{M}, D, A) \\ &\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + \Gamma_\perp(\mathcal{M}, D, A) \\ &\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') \in S) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + \gamma_\perp. \end{aligned}$$

For the final bullet-point, we need to consider every $S \subseteq \mathcal{R} \cup \{\perp\}$. Starting with $S = \perp$, we have

$$\begin{aligned}
\mathbb{P}(\mathcal{M}'_A(D) = \perp) &= \Gamma_\perp(\mathcal{M}, D, A) \\
&= e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) + \Gamma_\perp(\mathcal{M}, D, A) - e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) \\
&= e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') = \perp) + \Gamma_\perp(\mathcal{M}, D, A) - e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) \\
&\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') = \perp) + \gamma_\perp.
\end{aligned}$$

Now consider $S \subseteq \mathcal{R}$. We have

$$\begin{aligned}
\mathbb{P}(\mathcal{M}'_A(D) \in S) &\leq \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) \in S) \leq e^\varepsilon \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') \in S) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) \\
&\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) \\
&\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + e^\varepsilon \gamma_\perp + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp).
\end{aligned}$$

Now, considering $S' = S \cup \{\perp\}$ with $S \subseteq \mathcal{R} \cup \{\perp\}$, we have

$$\begin{aligned}
\mathbb{P}(\mathcal{M}'_A(D) \in S') &= \mathbb{P}(\mathcal{M}'_A(D) \in S) + \mathbb{P}(\mathcal{M}'_A(D) = \perp) \\
&\leq e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) \\
&\quad + e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D) = \perp) + \Gamma_\perp(\mathcal{M}, D, A) - e^\varepsilon \Gamma_\perp(\mathcal{M}, D', A) \\
&= e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + e^\varepsilon \mathbb{P}(\mathcal{M}'(D) = \perp) + \Gamma_\perp(\mathcal{M}, D, A) \\
&= e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S') + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + \Gamma_\perp(\mathcal{M}, D, A).
\end{aligned}$$

Again, this is at below $e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S') + \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) + e^\varepsilon \gamma_\perp$, given that $\Gamma_\perp(\mathcal{M}, D, A) \leq \gamma_\perp$. Thus the lemma follows. $\square$

Theorem 1. For $\text{leak} \subseteq \{\text{DB}\}$, all $\mathcal{M}, A, \text{VIEW}$ and all $D \in \mathcal{D}$ as above, $\mathcal{M}'_{A \neq \perp}(D) \sim \mathcal{M}(D)$. Furthermore, $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate.

Proof. Note that if $\text{leak} \subseteq \{\text{DB}\}$ then the abort probability is independent of the outcome. Therefore, for every $s \in \mathcal{R}$, we have $\mathbb{P}(\mathcal{M}'_A(D) = s) = (1 - \Gamma_\perp(\mathcal{M}, D, A))\mathbb{P}(\mathcal{M}(D) = s)$ and thus

$$\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) = s) = \frac{(1 - \Gamma_\perp(\mathcal{M}, D, A)) \cdot \mathbb{P}(\mathcal{M}(D) = s)}{1 - \Gamma_\perp(\mathcal{M}, D, A)} = \mathbb{P}(\mathcal{M}(D) = s).$$

$\square$

3.2 Useful Lemmas and Towards General Bounds

The results for difference leakage types and VIEW functions are not necessarily independent of each other. We start by showing that if one VIEW' (given leak') can be simulated from another VIEW (given leak) then DP claims of $\mathcal{M}'$ for $(\text{leak}, \text{VIEW})$ also apply to $\mathcal{M}'$ for $(\text{leak}', \text{VIEW}')$.

Definition 8. For a leakage type leak , it's associated domain leak_{dom} is the cartesian product of three sets. If $\text{DB} \in \text{leak}$ then the first set is $\mathcal{D}$ and otherwise

it is $\{\top\}$. If $\text{sample} \in \text{leak}$ then the second set is $\mathcal{R}$ and otherwise it is $\{\top\}$. If $\text{outcome} \in \text{leak}$ then the third set is $\mathcal{R}$ and otherwise it is $\{\top\}$.

For two leakage types $\text{leak}, \text{leak}'$, we say that $L \in \text{leak}_{\text{dom}}$ and $L' \in \text{leak}'_{\text{dom}}$ are corresponding, denoted $L \approx L'$, if for each $i \in \{1, 2, 3\}$, either $L_i = L'_i$ or $L_i = \top$ or $L'_i = \top$.

Lemma 2. *Let leak and leak' be leakage types. Let $\text{VIEW}, \text{VIEW}'$ be probabilistic functions to $\{0, 1\}^*$ from leak_{dom} and $\text{leak}'_{\text{dom}}$, respectively. Let $\mathcal{M}''$ be the aborting mechanism for $(\mathcal{M}, \text{leak}', \text{VIEW}')$ and let $\mathcal{M}'$ be for $(\mathcal{M}, \text{leak}, \text{VIEW})$.*

If $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP and there exists a probabilistic function $\Psi : \{0, 1\}^* \rightarrow \{0, 1\}^*$ such that $\Psi \circ \text{VIEW}(L) \sim \text{VIEW}'(L')$ for all corresponding $L \in \text{leak}_{\text{dom}}, L' \in \text{leak}'_{\text{dom}}$, then $\mathcal{M}''$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP. This applies also to $\mathcal{M}'_{\neq \perp}$ and $\mathcal{M}''_{\neq \perp}$.

Proof. Let A'' be an aborter in $\mathcal{M}''$ and L, L' be corresponding. Now let $A' := A'' \circ \Psi$ be an aborter in $\mathcal{M}'$. Clearly, $A' \circ \text{VIEW}(L) \sim A' \circ \text{VIEW}'(L')$ for all $L \approx L'$, and thus $\mathcal{M}'_{A'}(D) \sim \mathcal{M}''_{A''}(D)$ for all $D \in \mathcal{D}$. If $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP then $\mathcal{M}'_{A'}$, in particular, is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP. As $\mathcal{M}''_{A''}$ has the exact same distribution, it is also $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP. Since this holds for any A'' , it follows that $\mathcal{M}''$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP. Since $\mathcal{M}'_{A'}(D) \sim \mathcal{M}''_{A''}(D)$, clearly $\mathcal{M}'_{A' \neq \perp}(D) \sim \mathcal{M}''_{A'' \neq \perp}(D)$ so the above also holds for $\mathcal{M}'_{\neq \perp}$. $\square$

It appears reasonable that for most applications, it should be easy to find such a simulator Ψ for the minimal leakage type since analyzing the useful information content in the view of the adversary (aborter, in our restricted case) is typically already a part of the security argument.

Naturally, as the ‘goal’ of the aborter is to increase the privacy parameters of $\mathcal{M}'$, the aborter should get less powerful when it is given less information (the leakage type gets smaller). We confirm this in the lemma below. It implies a hierarchy where upper bounds on the DP and accuracy parameters for a leakage type leak' also applies to all strictly smaller types. Similarly, lower bounds on the DP parameters apply to all strictly larger leakage types.

Lemma 3 (Hierarchy lemma). *If $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP for $(\mathcal{M}, \text{leak}, \text{Id})$ and $\text{leak}' \subseteq \text{leak}$, then $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP for $(\mathcal{M}, \text{leak}', \text{Id})$. The same holds for $\mathcal{M}'_{\neq \perp}$.*

Proof. This follows from Lemma 2 in the special case of $\text{VIEW} = \text{VIEW}' = \text{Id}$. Let $L \in \text{leak}_{\text{dom}}$ and $L' \in \text{leak}'_{\text{dom}}$ be corresponding. A simulator Ψ trivially exists – it simply outputs L' when given L by omitting some elements. $\square$

Taken in the contrapositive, if $\text{leak}' \subseteq \text{leak}$ and $\mathcal{M}'$ is not $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP for $(\mathcal{M}, \text{leak}', \text{Id})$ then $\mathcal{M}'$ is not $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_{\perp}))$ -DP for $(\mathcal{M}, \text{leak}, \text{Id})$. Further, as one can derive the noise sample from the database together with the outcome, and the outcome from the database together with the noise sample, these leakage types should be equivalent. We confirm this as well.

Lemma 4. *With $\text{VIEW} = \text{Id}$, $\mathcal{M}'$ has the same DP parameters for $\text{leak} = \{\text{DB}, \text{sample}\}$, $\text{leak}' = \{\text{DB}, \text{outcome}\}$ and $\text{leak}'' = \{\text{DB}, \text{sample}, \text{outcome}\}$. The same holds for $\mathcal{M}'_{\neq \perp}$.*

Proof. By the hierarchy lemma, the DP parameters of $\mathcal{M}'$ for leak and leak' are no larger than those for leak'' . For the other directions, we apply Lemma 2 with $\text{VIEW} = \text{Id}$. The simulator Ψ when starting from leak takes as input $(D, z, \top)$ and outputs $(D, z, f(D) + z)$. The simulator Ψ' when starting from leak' takes as input $(D, \top, s)$ and outputs $(D, s - f(D), z)$. Thus, Lemma 2 implies that the privacy parameters of $\mathcal{M}'$ for leak and leak' are no smaller than those for leak'' . $\square$

We need also the following two observations.⁵ The proofs are deferred to Appendix A.

Proposition 1. *For every $\mathcal{M}, \text{leak}, A, \text{VIEW}$ and $D \in \mathcal{D}$ as above, we have $\mathcal{M}'_A(D) \approx_{\Gamma_{\perp}^{\max}(\mathcal{M}, A)}^s \mathcal{M}(D)$ and $\mathcal{M}'_{A \neq \perp}(D) \approx_{\Gamma_{\perp}^{\max}(\mathcal{M}, A)}^s \mathcal{M}(D)$.*

Lemma 5. *Let $\varepsilon \geq 0$ and $\eta, \delta \in [0, 1]$. For any two $\mathcal{M}_1, \mathcal{M}_2 : \mathcal{D} \rightarrow \mathcal{R}$, if $\mathcal{M}_1(D) \approx_{\eta}^s \mathcal{M}_2(D)$ for all $D \in \mathcal{D}$ and $\mathcal{M}_1$ is (ε, δ) -DP, then $\mathcal{M}_2$ is $(\varepsilon, \delta + (e^{\varepsilon} + 1)\eta)$ -DP.*

We are now ready to prove our general bounds for DP and accuracy.

Theorem 2 (General bound). *For every $\mathcal{M}, \text{leak}, A, \text{VIEW}$, both $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^{\varepsilon} + 1)\gamma_{\perp})$ -DP and the parameters are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$.*

Proof. For all A with $\Gamma_{\perp}^{\max}(\mathcal{M}, A) \leq \gamma_{\perp}$, Proposition 1 implies that $\mathcal{M}'_A(D) \approx_{\gamma_{\perp}}^s \mathcal{M}(D)$ for every $D \in \mathcal{D}$. Lemma 5 then implies that $\mathcal{M}'_A$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^{\varepsilon} + 1)\gamma_{\perp})$ -DP. The same holds for $\mathcal{M}'_{\neq \perp}$. The lower bounds follow from that for choices of $\gamma_{\perp}$, the aborter which never aborts is included in the set of considered aborter strategies and this aborter clearly leads to $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. $\square$

Proposition 2. *For every leak , $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$ are $(\alpha, \beta + \gamma_{\perp})$ -accurate.*

Proof. For every A with $\Gamma_{\perp}^{\max}(\mathcal{M}, A) \leq \gamma_{\perp}$, we have

$$\begin{aligned} \mathbb{P}(|\mathcal{M}'_A(D) - f(D)| > \alpha) &\leq \mathbb{P}(|\mathcal{M}(D) - f(D)| > \alpha) + SD(\mathcal{M}'_A(D), \mathcal{M}(D)) \\ &\leq \beta + \gamma_{\perp}, \end{aligned}$$

by Proposition 1. The same applies to $\mathcal{M}'_{\neq \perp}$ and thus the bound follows. $\square$

⁵ The effect of a statistical distance on the DP parameters (e.g. when approximating a DP mechanism) is used in many places in the literature, such as [43, 52, 7].

4 Improved Bounds in the Model of Aborts

For all of the bounds in this section, we restrict our attention to $\text{VIEW} = \text{Id}$. To derive bounds in the case of database-independent aborts, we use the idea of *mixture mechanisms* [50,4]. A mixture $\mathcal{M}_{\text{mix}}$ is the mechanism resulting from running a mechanism $\mathcal{M}_1$ with some fixed probability η and otherwise running some other mechanism $\mathcal{M}_2$. It is required that the choice of mechanism is independent of the database and the randomness otherwise used in the mechanisms. The DP parameters of the mixture are, roughly, the average of the parameters of $\mathcal{M}_1$ and $\mathcal{M}_2$ [50,4]. To get tighter bounds on this average, we use the hypothesis-testing formulation of DP [18,51].

Definition 9 ([18]). Let $T : [0, 1] \rightarrow [0, 1]$ be a convex, continuous and non-increasing function such that for all $x \in [0, 1]$, $T(x) \leq 1 - x$. A mechanism $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ is said to satisfy T -DP if for all adjacent $D, D' \in \mathcal{D}$ and all $x \in [0, 1]$: $\inf_{S \subseteq \mathcal{R}} \{1 - \mathbb{P}(\mathcal{M}(D) \in S) | \mathbb{P}(\mathcal{M}(D') \in S) \leq x\} \geq T(x)$.

Lemma 6 ([18,51]). A mechanism $\mathcal{M}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP iff it is $T_{\varepsilon, \delta_{\mathcal{M}}(\varepsilon)}$ -DP with $T_{\varepsilon, \delta_{\mathcal{M}}(\varepsilon)}(x) := \max\{0, 1 - \delta_{\mathcal{M}}(\varepsilon) - e^\varepsilon x, e^{-\varepsilon}(1 - \delta_{\mathcal{M}}(\varepsilon) - x)\}$.

Note that $(0, 0)$ -DP (perfect privacy) is equivalent to T -DP with $T(x) = 1 - x$.

Lemma 7 ([50]). For mixture $\mathcal{M}_{\text{mix}}$ of mechanisms $\{\mathcal{M}_i\}_{i=1, \dots, k}$ with trade-off functions $\{T_{\mathcal{M}_i}\}$ and associated probabilities $\{w_i\}$, the trade-off function for $\mathcal{M}_{\text{mix}}$ is no less than $\sum_i w_i T_{\mathcal{M}_i}(\cdot)$.

Lemma 8. Let $\mathcal{M}_{\text{mix}}$ be a mixture between an $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP mechanism $\mathcal{M}$ and a $(0, 0)$ -DP mechanism $\bar{\mathcal{M}}$, where $\bar{\mathcal{M}}$ is run with probability η . Then $\mathcal{M}_{\text{mix}}$ is $(\ln(e^\varepsilon - (e^\varepsilon - 1)\eta), (1 - \eta)\delta_{\mathcal{M}}(\varepsilon))$ -DP.

Proof. By the trade-off functions of $\mathcal{M}$ and $\bar{\mathcal{M}}$, and Lemma 7, we get that $\mathcal{M}_{\text{mix}}$ is T' -DP with

$$\begin{aligned} T'(x) &\geq \eta(1 - x) + (1 - \eta)T_{\varepsilon, \delta_{\mathcal{M}}(\varepsilon)}(x) \\ &= \eta(1 - x) + (1 - \eta) \cdot \max\{0, 1 - \delta_{\mathcal{M}}(\varepsilon) - e^\varepsilon x, e^{-\varepsilon}(1 - \delta_{\mathcal{M}}(\varepsilon) - x)\} \\ &\geq \max \begin{cases} 0, \\ (1 - \eta)(1 - \delta_{\mathcal{M}}(\varepsilon) - e^\varepsilon x) + \eta(1 - x), \\ (1 - \eta)e^{-\varepsilon}(1 - \delta_{\mathcal{M}}(\varepsilon) - x) + \eta(1 - x). \end{cases} \end{aligned}$$

The second case is equal to $1 - (e^\varepsilon - \eta e^\varepsilon + \eta)x - (1 - \eta)\delta_{\mathcal{M}}(\varepsilon)$, which suggests that $\mathcal{M}_{\text{mix}}$ is $T_{\varepsilon', \delta'}(\cdot)$ -DP with $\varepsilon' = \ln(e^\varepsilon - (e^\varepsilon - 1)\eta)$ and $\delta' = (1 - \eta)\delta_{\mathcal{M}}(\varepsilon)$. The third clause of the expression for $T_{\varepsilon', \delta'}$ -DP is $e^{-\varepsilon'}(1 - \delta' - x)$ and this is less than $(1 - \eta)e^{-\varepsilon}(1 - \delta_{\mathcal{M}}(\varepsilon) - x) + \eta(1 - x)$ for all values $\eta, x \in [0, 1]$ and thus $\mathcal{M}_{\text{mix}}$ is indeed $T_{\varepsilon', \delta'}$ -DP. $\square$

Note that $(\ln(e^\varepsilon - (e^\varepsilon - 1)\eta), \delta(\varepsilon))$ -DP for every privacy profile $\delta(\cdot)$ is equivalent to $(\varepsilon, \delta(\ln(\frac{e^\varepsilon - \eta}{1 - \eta})))$ -DP. Further, for every $\varepsilon \geq 0$ and every $\eta \in [0, 1)$,

we have $\ln(e^\varepsilon - (e^\varepsilon - 1)\eta) \leq \varepsilon \leq \ln\left(\frac{e^\varepsilon - \eta}{1 - \eta}\right)$. Thus $\delta(\varepsilon) \leq \delta\left(\ln\left(\frac{e^\varepsilon - \eta}{1 - \eta}\right)\right)$ since privacy profiles are monotone decreasing [4]. Let $\varepsilon^*(\varepsilon, \eta) := \ln(e^\varepsilon - (e^\varepsilon - 1)\eta)$ and $\bar{\varepsilon}(\varepsilon, \eta) := \ln\left(\frac{e^\varepsilon - \eta}{1 - \eta}\right)$, for $\eta \in [0, 1)$.

4.1 Fully Independent Aborts

For $\text{leak} = \{\}$, the probability of abort is independent of the database, i.e. $\Gamma_\perp(\mathcal{M}, D, A) = \Gamma_\perp^{\max}(\mathcal{M}, A)$. Thus $\mathcal{M}'_A$ can be formulated as a mixture mechanism and we can apply Lemma 8. Let $\mathcal{M}$ denote the constant mechanism which always outputs $\perp$ for every $D \in \mathcal{D}$.

Theorem 3. *For $\text{leak} = \{\}$, $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP.*

Proof. For $\text{leak} = \{\}$, the aborter A is given no input (or rather is always given $(\top, \top, \top)$) and hence every A is simply a Bernoulli trial with some fixed probability $\Gamma_\perp^{\max}$ of returning $\perp$. For every such $\Gamma_\perp^{\max} > 0$, $\mathcal{M}'_A$ is a mixture mechanism between $\mathcal{M}'_{A \neq \perp}$ and $\mathcal{M}$, where $\mathcal{M}$ is run with probability $\Gamma_\perp^{\max}$. By Theorem 1, $\mathcal{M}'_{A \neq \perp}$ is identically distributed to $\mathcal{M}$ and is thus $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. Hence, by Lemma 8 with $\eta = \Gamma_\perp^{\max}$, we get that $\mathcal{M}'_A$ is $(\varepsilon^*(\varepsilon, \Gamma_\perp^{\max}), (\Gamma_\perp^{\max})\delta_{\mathcal{M}}(\varepsilon))$ -DP, which is equivalent to $(\varepsilon, (1 - \Gamma_\perp^{\max})\delta_{\mathcal{M}}(\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})))$ -DP. Now note that $(1 - \Gamma_\perp^{\max})\delta_{\mathcal{M}}(\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max}))$ is strictly decreasing in $\Gamma_\perp^{\max}$. Hence for every upper bound $\gamma_\perp$ on $\Gamma_\perp^{\max}$, the largest DP parameters for $\mathcal{M}'_A$ are reached for $\Gamma_\perp^{\max} = 0$, i.e. the aborter that simply never aborts. Hence $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP $\square$

Given the general lower bound of $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP, we know that the upper bound on $\mathcal{M}'$ for $\text{leak} = \{\}$ is tight. Note that this does not imply that $\mathcal{M}'$ is (α, β) -accurate, which it generally is not. For $\mathcal{M}'_{\neq \perp}$, Theorem 1 implies that both privacy and accuracy parameters are exactly those of $\mathcal{M}$.

4.2 Dependence On Sample Only

For $\text{leak} = \{\text{sample}\}$, the abort probabilities are again independent of the database, so we can use the mixture-mechanism lemma.

Theorem 4. *For $\text{leak} = \{\text{sample}\}$, $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP with $\delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) = \max\{(1 - \Gamma_\perp^{\max}) \cdot (\delta_{\mathcal{M}}(\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})) + (e^{\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})} + 1)\Gamma_\perp^{\max}) : \Gamma_\perp^{\max} \leq \gamma_\perp\}$ and $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$ -DP.*

Proof. The upper bound for $\mathcal{M}'_{\neq \perp}$ is the general one (Theorem 2), so we turn to the upper bound for $\mathcal{M}'$. For every A , the view of A , consisting of only a noise sample, is independent of the database. Thus $\mathcal{M}'_A$ is a mixture between $\mathcal{M}'_{A \neq \perp}$ and $\mathcal{M}$ where $\mathcal{M}$ is run with probability $\Gamma_\perp^{\max}(\mathcal{M}, A)$. Thus Lemma 8 implies that $\mathcal{M}'_A$ is $(\varepsilon^*(\varepsilon, \Gamma_\perp^{\max}), (1 - \Gamma_\perp^{\max}) \cdot (\delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\Gamma_\perp^{\max}))$ -DP, which is equivalent to $(\varepsilon, (1 - \Gamma_\perp^{\max}) \cdot (\delta_{\mathcal{M}}(\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})) + (e^{\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})} + 1)\Gamma_\perp^{\max}))$ -DP. Hence, $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp))$ -DP with $\delta_{\mathcal{M}'}(\varepsilon, \gamma_\perp) = \max\{(1 - \Gamma_\perp^{\max}) \cdot (\delta_{\mathcal{M}}(\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})) + (e^{\bar{\varepsilon}(\varepsilon, \Gamma_\perp^{\max})} + 1)\Gamma_\perp^{\max}) : \Gamma_\perp^{\max} \leq \gamma_\perp\}$ -DP. $\square$

The specific privacy profile $\delta_{\mathcal{M}}$ and values of ε and $\gamma_{\perp}$ dictate whether $\max\{(1 - \Gamma_{\perp}^{max}) \cdot (\delta_{\mathcal{M}}(\varepsilon, \Gamma_{\perp}^{max})) + (e^{\varepsilon(\varepsilon, \Gamma_{\perp}^{max})} + 1)\Gamma_{\perp}^{max} : \Gamma_{\perp}^{max} \leq \gamma_{\perp}\}$ is above or below $\delta_{\mathcal{M}}(\varepsilon)$. For deriving the parameter regimes when it is above $\delta_{\mathcal{M}}(\varepsilon)$, i.e. aborts have an adversarial effect on the DP parameters, one needs a closed formula for $\delta_{\mathcal{M}}$. Thus such regimes must be separately derived for each target mechanism $\mathcal{M}$. We leave doing so for future work.

4.3 Dependence On Outcome Only

For $\text{leak} = \{\text{outcome}\}$, the abort probability is dependent on the database and thus we cannot apply the mixture-mechanism lemma. We can, however, apply the *post-processing lemma*.

Lemma 9 (Post-processing lemma [22,49]). *If $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ is (ε, δ) -DP and $F : \mathcal{R} \rightarrow \mathcal{R}'$ is any probabilistic function then $F \circ \mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}'$ is (ε, δ) -DP.*

It can be applied since the output of $\mathcal{M}'_A$ is equal to $A \circ \mathcal{M}$. Let *Geo* denote the two-sided geometric (discrete Laplace) [36,25] distribution over $\mathbb{Z}$. *Geo* with parameter $p \in (0, 1)$ has mass function $\mathbb{P}(\text{Geo}(p) = z) = \frac{1-p}{1+p} p^{|z|}$ and cumulative density function (cdf)

$$\mathbb{P}(\text{Geo}(p) \leq z) = \begin{cases} \frac{p^{-|z|}}{1+p}, & \text{if } z < 0, \\ 1 - \frac{p^{|z|+1}}{1+p}, & \text{otherwise.} \end{cases}$$

Theorem 5. *For $\text{leak} = \{\text{outcome}\}$, $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_{\perp})$ -DP. There is a mechanism $\mathcal{M}$ and a value $c_{\mathcal{M}} \in (0, 1)$ such that the parameters for $\mathcal{M}'_{\neq \perp}$ are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}} \cdot \gamma_{\perp})$.*

Proof. By the post-processing lemma, $\mathcal{M}'_A$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP for every A , so $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. Lemma 1 then implies that $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon} \gamma_{\perp})$ -DP. For the lower bounds, we consider the geometric mechanism. Let $\mathcal{R} = \mathbb{Z}$, f have an l_1 -sensitivity of 1 and let Z be *Geo*(p) with $p \in (0, 1)$. Then $\mathcal{M}$ is $(\varepsilon, 0)$ -DP for all $\varepsilon \geq \ln(1/p)$ [25]. WLOG, fix two adjacent $D, D' \in \mathcal{D}$ such that $f(D) = 0$ and $f(D') = 1$. Let A given an outcome s be such that it aborts iff $s \leq -1$, and thus $\Gamma_{\perp}^{max}(\mathcal{M}, A) = \Gamma_{\perp}(\mathcal{M}, D, A) = \mathbb{P}(Z \leq -1) = \frac{p^{-1}}{1+p}$, by the cdf of *Geo*(p). Then the support of $\mathcal{M}'_{A \neq \perp}$ is the non-negative integers and $\mathcal{M}'_{A \neq \perp}(D)$ has more mass

than $\mathcal{M}'_{A \neq \perp}(D')$ on 0 but less mass everywhere else. We get

$$\begin{aligned}
\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) = 0) &= \frac{\mathbb{P}(\mathcal{M}'_A(D) = 0)}{1 - \Gamma_{\perp}(D, A)} = \frac{\mathbb{P}(\mathcal{M}(D) = 0)}{1 - \Gamma_{\perp}(D, A)} = \frac{1}{p} \frac{\mathbb{P}(\mathcal{M}(D') = 0)}{1 - \Gamma_{\perp}(D, A)} \\
&= \frac{1}{p} \frac{\mathbb{P}(\mathcal{M}'_A(D') = 0)}{1 - \Gamma_{\perp}(D, A)} = \frac{1}{p} \frac{(1 - \Gamma_{\perp}(D', A)) \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0)}{1 - \Gamma_{\perp}(D, A)} \\
&= \frac{1}{p} \left(\frac{1 - \mathbb{P}(Z \leq -2)}{1 - \mathbb{P}(Z \leq -1)} \right) \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0) \\
&= \frac{1}{p} \left(1 + \frac{\mathbb{P}(Z = 1)}{1 - \mathbb{P}(Z \leq -1)} \right) \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0) \\
&= \frac{1}{p} \left(1 + \frac{\frac{(1-p)p}{1+p}}{1 - \Gamma_{\perp}^{max}(A)} \right) \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0) \\
&= \frac{1}{p} \left(1 + \frac{(1-p)p^2 \Gamma_{\perp}^{max}(A)}{1 - \Gamma_{\perp}^{max}(A)} \right) \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0).
\end{aligned}$$

Therefore, $\mathcal{M}'_{A \neq \perp}$ is $(\varepsilon, 0)$ -DP if only if $e^{\varepsilon} \geq \frac{1}{p} \left(1 + \frac{(1-p)p^2 \Gamma_{\perp}^{max}(A)}{1 - \Gamma_{\perp}^{max}(A)} \right) > \frac{1}{p} (1 + (1-p)p^2 \Gamma_{\perp}^{max}(A)) > \frac{1}{p}$. Furthermore, for the specific choice $\varepsilon = \ln(1/p)$, $\mathcal{M}'_{A \neq \perp}$ is not $(\varepsilon, 0)$ -DP (as $\mathcal{M}$ is) but rather the δ -parameters is no smaller than $\frac{1}{p} \frac{(1-p)p^2 \Gamma_{\perp}^{max}(A)}{1 - \Gamma_{\perp}^{max}(A)} \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0) > (1-p)p \cdot \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0) \cdot \Gamma_{\perp}^{max}(A)$, which is larger than 0 for every $p \in (0, 1)$. Now note that $(1-p)p \cdot \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D') = 0)$ lies strictly between 0 and 1, and is a function of only $\mathcal{M}$ and A . We denote it $c_{\mathcal{M}}$. Therefore, there exists a tuple $(\varepsilon, \mathcal{M}, A)$ such that $\mathcal{M}'_{A \neq \perp}$ cannot have better DP parameters than $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}} \cdot \gamma_{\perp})$, for a mechanism-specific constant $c_{\mathcal{M}} \in (0, 1)$. This proves the lower bound on the parameters for $\mathcal{M}'_{\neq \perp}$. $\square$

4.4 Database-dependent Aborts

Before analyzing $\text{leak} = \{\text{sample}, \text{outcome}\}$, we consider the case where $\text{DB} \in \text{leak}$. The general bound (Theorem 2) gives us that for any leakage type and any $\varepsilon, \delta_{\mathcal{M}}(\varepsilon)$, $\mathcal{M}'$ and $\mathcal{M}'_{\neq \perp}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^{\varepsilon} + 1)\gamma_{\perp})$ -DP. We now show that if $\text{DB} \in \text{leak}$ then this is essentially tight for $\mathcal{M}'$. We rely on the following lemma from [7]. For completeness, we include a proof in our notation in Appendix A.

Lemma 10 ([7]). *For $\text{leak} = \{\text{DB}\}$, the DP parameters of $\mathcal{M}'$ are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon} \cdot \gamma_{\perp})$.*

Note that Lemma 10 does not apply to $\mathcal{M}'_{\neq \perp}$, where Theorem 1 already shows $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP.

Theorem 6. *For $\text{leak} = \{\text{DB}\}$, $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon} \cdot \gamma_{\perp})$.*

Proof. By Theorem 1, $\mathcal{M}'_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and this implies, via Lemma 1, that $\mathcal{M}'$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^{\varepsilon} \gamma_{\perp})$ -DP. This meets the lower bound of Lemma 10. $\square$

Theorem 7. For $\text{leak} = \{\text{DB}, \text{sample}, \text{outcome}\}$, $\text{leak}' = \{\text{DB}, \text{sample}\}$ and $\text{leak}'' = \{\text{DB}, \text{outcome}\}$, the DP parameters of $\mathcal{M}'$ are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \cdot \gamma_\perp)$, and those for $\mathcal{M}'_{\neq \perp}$ by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}} \cdot \gamma_\perp)$.

Proof. Lemma 4 implies that $\mathcal{M}'$ for these three leakage types all satisfy exactly the same DP guarantees. The hierarchy lemma (Lemma 3) implies that the lower bound for $\mathcal{M}'$ from Lemma 10 applies to them. Similarly, for $\mathcal{M}'_{\neq \perp}$, Theorem 5 applies to them. $\square$

4.5 Dependence On Sample and Outcome

As one can derive $f(D)$ from the sample z and outcome $s = f(D) + z$, it should make little difference if an aborter is given only (z, s) or if they are also given D . We show that this is true unless the target mechanism $\mathcal{M}$ is trivial in the sense that its output distribution does not depend on the database. For additive-noise mechanisms, triviality means that $f(D) = f(D')$ for all adjacent $D, D' \in \mathcal{D}$.

Theorem 8. For $\text{leak} = \{\text{sample}, \text{outcome}\}$, the parameters for $\mathcal{M}'_{\neq \perp}$ are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}} \cdot \gamma_\perp)$, for some $c_{\mathcal{M}} \in (0, 1)$. Unless $\mathcal{M}$ is trivial, those for $\mathcal{M}'$ by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \cdot \gamma_\perp)$.

Proof. The lower bound for $\mathcal{M}'_{\neq \perp}$ follows by the hierarchy lemma together with Theorem 5. For the lower bound for $\mathcal{M}'$, assume that $\mathcal{M}$ is non-trivial and hence there exists two adjacent D, D' such that $f(D) \neq f(D')$. Set $r = f(D')$ and let A compute $r' \leftarrow s - z$ when given (z, s) . Let A abort with probability $\gamma_\perp$ if $r' = r$ and with probability 0 otherwise. We get that $\Gamma_\perp(\mathcal{M}, D', A) = \gamma_\perp \geq 0$ and $\Gamma_\perp(\mathcal{M}, D, A) = 0$ for all $D \neq D'$. Now let $S \subseteq \mathcal{R}$ be such $\mathbb{P}(\mathcal{M}(D) \in S) = e^\varepsilon \mathbb{P}(\mathcal{M}(D') \in S) + \delta_{\mathcal{M}}(\varepsilon)$. Thus, we have that $\mathbb{P}(\mathcal{M}'_A(D') \in S) = \mathbb{P}(\mathcal{M}(D') \in S) - \gamma_\perp$ and $\mathbb{P}(\mathcal{M}'_A(D) \in S) = \mathbb{P}(\mathcal{M}(D) \in S)$. This implies

$$\begin{aligned} \mathbb{P}(\mathcal{M}'_A(D) \in S) &= \mathbb{P}(\mathcal{M}(D) \in S) = e^\varepsilon \mathbb{P}(\mathcal{M}(D') \in S) + \delta_{\mathcal{M}}(\varepsilon) \\ &= e^\varepsilon (\mathbb{P}(\mathcal{M}'_A(D') \in S) + \gamma_\perp) + \delta_{\mathcal{M}}(\varepsilon) \\ &= e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp. \end{aligned}$$

Therefore $\mathcal{M}'$ is not (ε, δ') -DP for any $\delta' < \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$. $\square$

5 DP and Accuracy of Ideal Protocol Executions

Within a protocol where multiple parties contribute parts of a database, we will distinguish between inputs given by the honest parties and those given by the corrupted ones. As we consider only static corruptions, the sets of honest and corrupted parties are fixed beforehand. Let $\mathcal{D}_H$ and $\mathcal{D}_C$ denote the domains for the inputs from the honest and corrupted parties, respectively. The target mechanism $\mathcal{M}$ is then from $\mathcal{D} := \mathcal{D}_C \times \mathcal{D}_H$ to $\mathcal{R}$. From each such mechanism $\mathcal{M}$ we can define a family of mechanisms indexed by the inputs from the corrupted parties. Let $\mathcal{M}_{\bar{D}_C}(\cdot) := \mathcal{M}(\bar{D}_C, \cdot)$ for each $\bar{D}_C \in \mathcal{D}_C$ and note that $\mathcal{M}_{\bar{D}_C}(D_H) \sim \mathcal{M}(\bar{D}_C, D_H)$ for every $D_H \in \mathcal{D}_H$.

Definition 10. We say that $\mathcal{M} : \mathcal{D}_C \times \mathcal{D}_H \rightarrow \mathcal{R}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP with respect to D_H if for every $\bar{D}_C \in \mathcal{D}_C$, $\mathcal{M}_{\bar{D}_C} : \mathcal{D}_H \rightarrow \mathcal{R}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP.

As to avoid confusion, we say that $\mathcal{M}$ is DP with respect to $\bar{D} \in \mathcal{D}$ when we speak of it being DP in the usual sense (i.e. for an adjacency notion over $\mathcal{D}$).

Lemma 11. If $\mathcal{M} : \mathcal{D}_H \times \mathcal{D}_C \rightarrow \mathcal{R}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP with respect to $\bar{D} \in \mathcal{D}$ then $\mathcal{M}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP with respect to D_H .

Proof. For every $\bar{D}_C \in \mathcal{D}_C$, if $D_H, D'_H \in \mathcal{D}_H$ are adjacent then $\bar{D} = (\bar{D}_C, D_H) \in \mathcal{D}$ and $\bar{D}' = (\bar{D}_C, D'_H) \in \mathcal{D}$ are also adjacent. Hence, for every $S \subseteq \mathcal{R}$, we have

$$\begin{aligned} \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) \in S) &= \mathbb{P}(\mathcal{M}(\bar{D}_C, D_H) \in S) \leq e^\varepsilon \mathbb{P}(\mathcal{M}(\bar{D}_C, D'_H) \in S) + \delta_{\mathcal{M}}(\varepsilon) \\ &= e^\varepsilon \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D'_H) \in S) + \delta_{\mathcal{M}}(\varepsilon). \end{aligned}$$

Hence every $\mathcal{M}_{\bar{D}_C}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. $\square$

5.1 Ideal Execution with Aborts

We recall the ideal protocol execution for security-with-abort.

Definition 11 ([27,39]). The ideal execution with abort is as follows.

1. **Inputs:** Each honest party P_i sends their input $\bar{D}_i = D_i$ to $\mathcal{F}_{\mathcal{M}}$. Each corrupted party P_j sends some input $\bar{D}_j$ to $\mathcal{F}_{\mathcal{M}}$.
2. **Early abort:** $\mathcal{F}_{\mathcal{M}}$ sends **abort?** to the adversary $\mathcal{S}$. If $\mathcal{S}$ answers $\top$ then $\mathcal{F}_{\mathcal{M}}$ continues, else it aborts (sends $\perp$ to all honest parties and halts).
3. **Compute:** Let $\bar{D} \leftarrow (\bar{D}_1, \dots, \bar{D}_n)$. $\mathcal{F}_{\mathcal{M}}$ computes $s \leftarrow \mathcal{M}(\bar{D})$.
4. **Late abort:** $\mathcal{F}_{\mathcal{M}}$ sends **(abort?, s)** to $\mathcal{S}$. If $\mathcal{S}$ answers $\top$ then $\mathcal{F}_{\mathcal{M}}$ continues and otherwise it aborts.
5. **Output:** $\mathcal{F}_{\mathcal{M}}$ sends s to each honest party.

This ideal execution, for a given $\mathcal{M}$ and $\mathcal{S}$ (controlling the corrupted parties) defines three randomized mappings that we are interested in. We refer to the outputs given to the honest parties as the public output and denote it $\text{Out}^{\mathcal{S}}(\bar{D})$.

First is the view of $\mathcal{S}$, i.e. the concatenation of its internal randomness, the inputs of the corrupted parties, and the set of messages $\mathcal{S}$ receives throughout the interaction. The set of messages that $\mathcal{S}$ receives do not depend on the inputs of the honest parties, except for the message it receives in step four. Therefore, the view of $\mathcal{S}$ can be generated (or simulated, as in the sense of Lemma 2) from only $s \leftarrow \mathcal{M}_{\bar{D}_C}(D_H)$. Therefore, roughly, the view of $\mathcal{S}$ corresponds to the VIEW function in the MoA, and each $\mathcal{S}$ then corresponds to some aborter A .

Second is the mapping from the used database $\bar{D}$ to the public output. This output is equal to $s \leftarrow \mathcal{M}(\bar{D})$ unless $\mathcal{S}$ decides to abort, given its view. Therefore this mapping also corresponds to the aborting mechanism $\mathcal{M}'_A$ in the MoA, with some A corresponding to $\mathcal{S}$.

Third is the mapping from the honest parties' inputs D_H to the public output. Assume, WLOG, that the corrupted parties have lower indices than the honest

ones and thus $\bar{D} = \bar{D}_C || D_H$. Then, as explained above, $\mathcal{M}(\bar{D}_C, \cdot)$ is equivalent to some $\mathcal{M}_{\bar{D}_C}$, which also is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP. That is, $\mathcal{S}$ has the power to freely chose one out of a family of $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP mechanisms. The public output is equal to $s \leftarrow \mathcal{M}_{\bar{D}_C}(D_H)$ unless $\mathcal{S}$ decides to abort (given its view). Therefore also this mapping corresponds to an aborting mechanism $\mathcal{M}'_A$. We now make these remarks formal.

Lemma 12. *For every $\mathcal{M}$ and every $\mathcal{S}$ in the ideal execution with aborts, there exists an aborter strategy A such that for every $\bar{D} \in \mathcal{D}$, we have $\text{Out}^{\mathcal{S}}(\bar{D}) \sim \mathcal{M}'_A(\bar{D})$ with $\mathcal{M}'$ being for $(\mathcal{M}, \{\text{DB}, \text{outcome}\}, \text{Id})$.*

Proof. The adversary $\mathcal{S}$ consists of two probabilistic algorithms. First, $\mathcal{S}_1 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run during step two and is given input $\bar{D}_C$. Second, $\mathcal{S}_2 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run in step four, unless $\mathcal{S}_1(\bar{D}_C) = \perp$, and is given $(\bar{D}_C, s)$ as input. Let $p_1(\bar{D}_C) := \mathbb{P}(\mathcal{S}_1(\bar{D}_C) = \perp)$ and $p_2(\bar{D}_C, s) := \mathbb{P}(\mathcal{S}_2(\bar{D}_C, s) = \perp)$. Then we get

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(\bar{D}) = \perp) = p_1(\bar{D}_C) + (1 - p_1(\bar{D}_C)) \cdot \sum_{s \in \mathcal{R}} p_2(\bar{D}_C, s) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s),$$

and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(\bar{D}) = s) = (1 - p_1(\bar{D}_C)) \cdot (1 - p_2(\bar{D}_C, s)) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s).$$

Now let $\text{leak} = \{\text{DB}, \text{outcome}\}$ in the MoA, which makes $L = (\bar{D}, \top, s)$. We construct A in two stages. First, $A_{\text{pre}}(L)$ returns $(\bar{D}_C, s)$ with probability $1 - p_1(\bar{D}_C)$, otherwise returning $\perp$. Then A_{post} takes as input the output of A_{pre} , and we set $A_{\text{post}}(\perp) = \perp$ and $A_{\text{post}}(v) = \mathcal{S}_2(v)$ for all $v \neq \perp$. Define $A := A_{\text{post}} \circ A_{\text{pre}}$. Then we get

$$\mathbb{P}(\mathcal{M}'_A(\bar{D}) = \perp) = p_1(\bar{D}_C) + (1 - p_1(\bar{D}_C)) \cdot \sum_{s \in \mathcal{R}} p_2(\bar{D}_C, s) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s).$$

For all $s \in \mathcal{R}$, we get

$$\mathbb{P}(\mathcal{M}'_A(\bar{D}) = s) = (1 - p_1(\bar{D}_C)) \cdot (1 - p_2(\bar{D}_C, s)) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s).$$

□

We also need a corresponding lemma for $\text{Out}^{\mathcal{S}}$ w.r.t. D_H . Due to similarities in the proofs, we defer the proof to Appendix A.

Lemma 13. *For every $\mathcal{M}_{\bar{D}_C}$ as above and every $\mathcal{S}$ in the ideal execution with aborts, there exists an aborter strategy A such that for every $D_H \in \mathcal{D}_H$, we have $\text{Out}^{\mathcal{S}}(D_H) \sim \mathcal{M}'_A(D_H)$ with $\mathcal{M}'$ being for $(\mathcal{M}_{\bar{D}_C}, \{\text{outcome}\}, \text{Id})$.*

Given these lemmas, we can apply the bounds from Section 4.

Theorem 9. *Let $\varepsilon, \alpha \geq 0$ and $\gamma_{\perp}, \beta \in [0, 1)$, and let $\mathcal{M} : \mathcal{D}_H \times \mathcal{D}_C \rightarrow \mathcal{R}$ be $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate. Under the assumption that $\mathcal{S}$ aborts with probability at most $\gamma_{\perp}$, the ideal execution with abort fulfills the following:*

- The view of $\mathcal{S}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H .
- $\text{Out}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H and $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$ -DP w.r.t. $\bar{D}$.
- $\text{Out}_{\neq \perp}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_\perp)$ -DP w.r.t. D_H and $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$ -DP w.r.t. $\bar{D}$.
- $\text{Out}^{\mathcal{S}}$ and $\text{Out}_{\neq \perp}^{\mathcal{S}}$ are $(\alpha, \beta + \gamma_\perp)$ -accurate w.r.t. $\bar{D}$.

Proof. The view of $\mathcal{S}$ consists of internal randomness, $\bar{D}_C$ and, unless they early abort, $\mathcal{M}_{\bar{D}_C}(D_H)$. By Lemma 11, each $\mathcal{M}_{\bar{D}_C}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP with respect to D_H . Both $\bar{D}_C$ and the internal randomness are independent of D_H and thus, the view of $\mathcal{S}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H . Regarding the public output $\text{Out}^{\mathcal{S}}$, Lemma 13 gives that $\text{Out}^{\mathcal{S}}(D_H) \sim \mathcal{M}'_A(D_H)$ for every $D_H \in \mathcal{D}_H$, with $\mathcal{M}'$ being for $(\mathcal{M}_{\bar{D}_C}, \{\text{outcome}\}, \text{Id})$. Therefore Theorem 5 implies that $\text{Out}^{\mathcal{S}}$ and $\text{Out}_{\neq \perp}^{\mathcal{S}}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + \gamma_\perp)$ -DP w.r.t. D_H , respectively. Furthermore, Lemma 12 implies that $\text{Out}^{\mathcal{S}}(\bar{D}) \sim \mathcal{M}'_A(\bar{D})$, with $\mathcal{M}'$ being for $(\mathcal{M}, \{\text{DB}, \text{outcome}\}, \text{Id})$. Hence, $\text{Out}^{\mathcal{S}}$ and $\text{Out}_{\neq \perp}^{\mathcal{S}}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)\gamma_\perp)$ -DP w.r.t. $\bar{D}$, by Theorem 2. Similarly, Proposition 2 implies the accuracy claims. $\square$

Remark 1. Importantly, lower bounds in the MoA also apply. In particular, the parameters for $\text{Out}_{\neq \perp}^{\mathcal{S}}$ with respect to either database are lower-bounded by $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + c_{\mathcal{M}}\gamma_\perp)$ for some $c_{\mathcal{M}} \in (0, 1)$, by Theorem 5.

5.2 Ideal Execution with Fairness

Definition 12. *The ideal execution with fairness is defined exactly as the one for security-with-abort but with the ‘Late abort’-step removed.*

Again, we need lemmas enabling us to apply results from the MoA and we defer the proofs to Appendix A due to similarity.

Lemma 14. *For every $\mathcal{M}$ and every $\mathcal{S}$ in the ideal execution with fairness, there exists an aborter strategy A such that for every $\bar{D} \in \mathcal{D}$, we have $\text{Out}^{\mathcal{S}}(\bar{D}) \sim \mathcal{M}'_A(\bar{D})$, with $\mathcal{M}'$ being for $(\mathcal{M}, \{\text{DB}\}, \text{Id})$.*

Lemma 15. *For every $\mathcal{M}_{\bar{D}_C}$ and every $\mathcal{S}$ in the ideal execution with fairness, there exists an aborter strategy A such that for every $D_H \in \mathcal{D}_H$, we have $\text{Out}^{\mathcal{S}}(D_H) \sim \mathcal{M}'_A(D_H)$, with $\mathcal{M}'$ being for $(\mathcal{M}_{\bar{D}_C}, \{\}, \text{Id})$.*

Theorem 10. *Let $\varepsilon, \alpha \geq 0$ and $\gamma_\perp, \beta \in [0, 1]$, and let $\mathcal{M} : \mathcal{D}_H \times \mathcal{D}_C \rightarrow \mathcal{R}$ be $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate. Under the assumption that $\mathcal{S}$ aborts with probability at most $\gamma_\perp$, the ideal execution with fairness fulfills the following:*

- The view of $\mathcal{S}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H .
- $\text{Out}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H and $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$ -DP w.r.t. $\bar{D}$.
- $\text{Out}_{\neq \perp}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and w.r.t. both D_H and $\bar{D}$.
- $\text{Out}^{\mathcal{S}}$ is $(\alpha, \beta + \gamma_\perp)$ -accurate and $\text{Out}_{\neq \perp}^{\mathcal{S}}$ is (α, β) -accurate w.r.t. $\bar{D}$.

Proof. The only part of the view of $\mathcal{S}$ which is not independent of D_H is $\mathcal{M}_{\bar{D}_C}(D_H)$. Since $\mathcal{M}_{\bar{D}_C}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP, by Lemma 11, we get that the view of $\mathcal{S}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H . By Lemma 15 we get that there exists some A such that $\text{Out}^{\mathcal{S}}(D_H) \sim \mathcal{M}'_A(D_H)$ for every $D_H \in \mathcal{D}_H$, with $\mathcal{M}'$ being for $(\mathcal{M}_{\bar{D}_C}, \{\}, \text{Id})$. Therefore Theorems 3 and 1 imply that $\text{Out}^{\mathcal{S}}$ and $\text{Out}^{\mathcal{S}}_{\neq \perp}$ are both $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H . Further, Lemma 14 implies that there exists some A such that $\text{Out}^{\mathcal{S}}(\bar{D}) \sim \mathcal{M}'_A(\bar{D})$ for every $\bar{D} \in \mathcal{D}$, with $\mathcal{M}'$ being for $(\mathcal{M}, \{\text{DB}\}, \text{Id})$. Hence, Theorem 6 implies that $\text{Out}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$ -DP w.r.t. $\bar{D}$ and Theorem 1 implies that $\text{Out}^{\mathcal{S}}_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. $\bar{D}$. Similarly, Proposition 2 implies the accuracy for $\text{Out}^{\mathcal{S}}$ and Theorem 1 that for $\text{Out}^{\mathcal{S}}_{\neq \perp}$. $\square$

This shows that in the ideal execution, fairness results in stronger privacy and accuracy guarantees than SwA, for most considered mappings. Particularly, with fairness, $\text{Out}^{\mathcal{S}}_{\neq \perp}$ has the same DP and accuracy properties as $\mathcal{M}$, whereas this is not the case for SwA. The fairness results for $\text{Out}^{\mathcal{S}}_{\neq \perp}$ further imply that as long as an honest party never publishes aborting outcomes, they are guaranteed that whatever they release comes from a mapping with the desired DP properties.

5.3 Two-party Solitary Output Functionalities

We now consider a case where the parties explicitly have different roles – solitary output functionalities (SOFs) [35,3]. We focus on the two-party case and say that a two-party functionality is SOF if only one specified party (called the *receiver*) gets an output. We further restrict that the database comes solely from the other party (called the *sender*). Note that, for SOFs, the ideal executions with fairness and abort are equivalent, since the sender never gets any output [35]. SOFs have several advantages over general two-party functionalities; For one, SOFs can be securely realized also in the two-party case, where achieving fairness is generally impossible [15]. We now show that SOFs give stronger DP and accuracy guarantees than SwA. We re-define the public output $\text{Out}^{\mathcal{S}}$ of a SOF to be the output given to the receiver, regardless of which party is corrupted.

Theorem 11. *Let $\varepsilon, \alpha \geq 0$ and $\gamma_\perp, \beta \in [0, 1)$, and let $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ be $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate. Under the assumption that $\mathcal{S}$ aborts with probability at most $\gamma_\perp$, the ideal protocol execution for SOFs satisfies the following.*

- *If the sender is corrupted then $\text{Out}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$ -DP, and $(\alpha, \beta + \gamma_\perp)$ -accurate, w.r.t. $\bar{D}$. $\text{Out}^{\mathcal{S}}_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate w.r.t. $\bar{D}$.*
- *If the receiver is corrupted then its view, $\text{Out}^{\mathcal{S}}$, and $\text{Out}^{\mathcal{S}}_{\neq \perp}$ are $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. $D_H = \bar{D}$. $\text{Out}^{\mathcal{S}}$ is $(\alpha, \beta + \gamma_\perp)$ -accurate and $\text{Out}^{\mathcal{S}}_{\neq \perp}$ is (α, β) -accurate.*

Proof. Let $\mathcal{S}$ be the corrupted sender. Lemma 14 implies that there exists some A such that $\text{Out}^{\mathcal{S}}(\bar{D}) \sim \mathcal{M}'_A(\bar{D})$ for every $\bar{D} \in \mathcal{D}$, with $\mathcal{M}'$ being for $(\mathcal{M}, \{\text{DB}\}, \text{Id})$. Hence, Theorem 6 implies that $\text{Out}^{\mathcal{S}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp)$ -DP w.r.t. $\bar{D}$ and Theorem 1 implies that $\text{Out}^{\mathcal{S}}_{\neq \perp}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. $\bar{D}$. The accuracy claims thus follow by Proposition 2 and Theorem 1, respectively.

Now let $\mathcal{S}$ be the corrupted receiver. The only part of the view of $\mathcal{S}$ which is dependent on $\bar{D} = D_H$ is the output $\mathcal{S}$ receives, and $\mathcal{S}$ must choose whether to abort based on no information about D_H or the mechanism execution. By Lemma 15 we get that there exists some A such that $\text{Out}^{\mathcal{S}}(D_H) \sim \mathcal{M}'_A(D_H)$ for every $D_H \in \mathcal{D}_H = \mathcal{D}$, with $\mathcal{M}'$ being for $(\mathcal{M}_{\mathcal{D}_C}, \{\}, \text{Id})$. Therefore Theorems 3 and 1 imply that $\text{Out}^{\mathcal{S}}$ and $\text{Out}^{\mathcal{S}}_{\neq \perp}$ are both $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H . Hence, also the view of $\mathcal{S}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP w.r.t. D_H . Accuracy again follows by Proposition 2 and Theorem 1. $\square$

6 DP and Accuracy of MPC protocols

The results from the previous section give us a way to analyze protocols that emulate the respective ideal executions. The ideal functionalities can be realized under different guarantees, such as against computational or statistical adversaries, and with varying bounds on closeness between the ideal and real executions. For relating the the guarantees of protocols to those of their respective ideal executions, we only need to know how computational and statistical distances influence accuracy and DP guarantees. We already know that:

- If two mechanism ensembles $\mathcal{M}_1, \mathcal{M}_2$ are have negligible statistical distance for every input and $\mathcal{M}_1$ is (ε, δ) -DP then $\mathcal{M}_2$ is $(\varepsilon, \delta + \text{negl})$ -DP. (Lemma 5)
- If two mechanism ensembles $\mathcal{M}_1, \mathcal{M}_2$ are have negligible computational distance for every input and $\mathcal{M}_1$ is (ε, δ) -DP then $\mathcal{M}_2$ is (ε, δ) -SIM-CDP. (Definition 3)

For accuracy, it is easy to see that if $\mathcal{M}_1, \mathcal{M}_2$ have a statistical distance below η for every input and $\mathcal{M}_1$ is (α, β) -accurate then $\mathcal{M}_2$ is $(\alpha, \beta + \eta)$ -accurate. Since we assume that all elements of $\mathcal{R}$ are of polynomial size in the security parameter, the same also holds for computational distance, which we now prove.

Proposition 3. *Let $\eta, \beta \in [0, 1], \alpha \geq 0$, and let $\mathcal{M}_1$ and $\mathcal{M}_2$ be mechanisms from $\mathcal{D}$ to $\mathcal{R} \cup \{\perp\}$. If $\mathcal{M}_1$ is (α, β) -accurate for $f : \mathcal{D} \rightarrow \mathcal{R}$ and $\mathcal{M}_1(D) \approx_{\eta}^c \mathcal{M}_2(D)$ for all $D \in \mathcal{D}$, then $\mathcal{M}_2$ is $(\alpha, \beta + \eta)$ -accurate for f .*

Proof. That $\mathcal{M}_1$ is accurate implies for all $D \in \mathcal{D}$ that $\mathbb{P}(|f(D) - \mathcal{M}_1(D)| \geq \alpha) \leq \beta$. For every $s \in \mathcal{R}$, it can be tested in polynomial time whether $|s - \mathcal{M}_1(D)| \geq \alpha$, since s is polynomial-sized. Thus $\mathbb{P}(|f(D) - \mathcal{M}_2(D)| \geq \alpha) \leq \mathbb{P}(|f(D) - \mathcal{M}_1(D)| \geq \alpha) + CD(\mathcal{M}_1(D), \mathcal{M}_2(D)) \leq \beta + \eta$. $\square$

6.1 Computational or Statistical Security with Aborts or Fairness

A protocol Π securely realizing an ideal functionality $\mathcal{F}_{\mathcal{M}}$ means that the joint distribution of the view of the adversary and the honest parties' outputs between the ideal execution and the protocol in the real world have negligible computational distance [27,39]. This means that the adversarial view, and public output, each separately are computationally indistinguishable between the

worlds. Hence, if the adversarial view in the ideal execution is (ε, δ) -DP then the adversarial view in the real one is (ε, δ) -SIM-CDP.⁶ The same applies for the public output. The accuracy results carries over from the ideal to the real world due to Proposition 3, with a negligible increase in β . Therefore, we directly get the following.

Corollary 1. *If Π securely realizes $\mathcal{F}_{\mathcal{M}}$ (with abort, fairness, or for a SOF) against PPT adversaries, then Π satisfies the corresponding results in Table 2 but with SIM-CDP instead of DP, and with a negligible increase in β .*

The same holds in the statistical case, but instead of DP turning computational, there is a negligible increase in δ .⁷

Corollary 2. *If Π securely realizes $\mathcal{F}_{\mathcal{M}}$ (with abort, fairness, or for a SOF) against unbounded adversaries, then Π satisfies the corresponding results in Table 2 but with a negligible increase in δ and β .*

6.2 Partially Fair Two-party Computation

Fairness cannot be achieved for general randomized functionalities whenever a majority of the parties can be corrupted [15], which includes the two-party case. For instance, any dishonest-majority r -round protocol for coin-tossing will have a bias of at least $\Omega(1/r)$. It is possible to meet this bound for coin-tossing [46] and also for general randomized functionalities, as shown by Gordon and Katz [29]. This means that one, with computational security, can get the bias (computational distance between outputs of the ideal and real executions) down to $1/p$ for any p polynomial in the security parameter. Gordon-Katz formalizes partial fairness in terms of $1/p$ -security.⁸

Definition 13 ([29]). *For a function $p : \mathbb{N} \rightarrow \mathbb{R}_+$, a protocol Π is said to $1/p$ -securely compute $\mathcal{F}$ if for every PPT real-world adversary $\mathcal{A}$, there is a PPT adversary $\mathcal{S}$ in the fair ideal world such that $\text{Ideal}_{\mathcal{F}, \mathcal{A}}(D_1, D_2) \approx_{1/p}^c \text{Real}_{\Pi, \mathcal{S}}(D_1, D_2)$.*

Gordon-Katz constructs, for arbitrary randomized functionalities, a protocol which is $1/p$ -secure, assuming the existence of enhanced trapdoor permutations [27].⁹ We now prove that partial fairness ($1/p$ -security) results in DP and accuracy guarantees quite similar to those of full fairness. For this, we need a way to bound the effects that a non-negligible computational distance have on DP parameters. To enable this, we consider IND-CDP instead of SIM-CDP, and use the following lemma.

⁶ This can alternatively be proven via SIM^+ -CDP [45], as it per definition is fulfilled by these protocols and it is known to imply SIM-CDP in the adversarial view.

⁷ In both cases, there is an increase of $(e^\varepsilon + 1) \cdot \text{negl}(\kappa)$ in the δ -parameter. For SIM-CDP, this may be absorbed into the negligible slack inherent in the definition.

⁸ The notion of $1/p$ -security was later generalized to the multiparty setting [5], though we only study it in the two-party case.

⁹ The protocol requires that either the range or at least one of the domains of $\mathcal{F}$ is polynomial-sized. Note that, for the DP functionality $\mathcal{F}_{\mathcal{M}}$, there is no inherent need to have the range of the functionality grow in the security parameter.

Lemma 16 ([43,10]). For $\eta \in (0, 1)$ and every two distributions X, Y on $\mathcal{R}$, if $X \approx_{\eta}^c Y$ then there exists a third distribution Z on $\mathcal{R}$ and negligible function negl such that $Z \approx_{\eta}^s Y$ and $X \approx_{\text{negl}}^c Z$.

This implies that if $\mathcal{M}_1(D)$ has computational distance $1/p(\kappa)$ to $\mathcal{M}_2(D)$ for every D , and $\mathcal{M}_1(D)$ is (ε, δ) -DP then $\mathcal{M}'$ is $(\varepsilon, \delta + (e^\varepsilon + 1)/p)$ -IND-CDP. It is open if a similar result can be obtained for SIM-CDP [43]. Recall that $\mathcal{A}$ is the real-world adversary. We let $\text{Out}^{\mathcal{A}}$ denote the public output in the real world.

Theorem 12. Let $\varepsilon, \alpha \geq 0$ and $\gamma_{\perp}, \beta \in [0, 1)$, and let $\mathcal{M} : \mathcal{D}_H \times \mathcal{D}_C \rightarrow \mathcal{R}$ be $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon))$ -DP and (α, β) -accurate. Under the assumption that $\mathcal{A}$ aborts with probability at most $\gamma_{\perp}$, any protocol Π which realizes $\mathcal{F}_{\mathcal{M}}$ with $1/p$ -security fulfills the following.

- The view of $\mathcal{A}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)/p(\kappa))$ -IND-CDP w.r.t. D_H .
- $\text{Out}^{\mathcal{A}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)/p(\kappa))$ -IND-CDP w.r.t. D_H and $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_{\perp} + (e^\varepsilon + 1)/p(\kappa))$ -IND-CDP w.r.t. $\bar{D}$.
- $\text{Out}_{\neq \perp}^{\mathcal{A}}$ is $(\varepsilon, \delta_{\mathcal{M}}(\varepsilon) + (e^\varepsilon + 1)/p(\kappa))$ -IND-CDP w.r.t. both D_H and $\bar{D}$.
- $\text{Out}^{\mathcal{A}}$ is $(\alpha, \beta + \gamma_{\perp} + 1/p(\kappa))$ -accurate and $\text{Out}_{\neq \perp}^{\mathcal{A}}$ is $(\alpha, \beta + 1/p(\kappa))$ -accurate, both w.r.t. $\bar{D}$.

Proof. That Π is $1/p$ -secure implies that the view of $\mathcal{A}$ has computational distance at most $1/p(\kappa)$ to the view of $\mathcal{S}$ in the fair ideal world, and similarly that $\text{Out}^{\mathcal{A}}$ and $\text{Out}^{\mathcal{S}}$ have computational distance at most $1/p(\kappa)$, for every input database. Hence Lemma 16 implies that $\text{Out}^{\mathcal{A}}$, $\text{Out}_{\neq \perp}^{\mathcal{A}}$ and the view of $\mathcal{A}$ each are IND-CDP with the same parameters as their corresponding mapping in the fair ideal execution, but with each δ -parameter increased by $(e^\varepsilon + 1)/p(\kappa)$. All the IND-CDP claims then follow from Theorem 10. For accuracy, Proposition 3 implies that each mapping in the real world satisfies the same accuracy guarantees as in the fair ideal world, but with the β 's increased by $1/p(\kappa)$. Therefore $1/p$ -security together with Theorem 10 implies the accuracy claims. $\square$

We see that a partially fair protocol satisfies the same guarantees as a fully fair one but with IND-CDP instead of SIM-CDP and with an arbitrarily small (but non-negligible) increase in the δ and β parameters. In particular, partial fairness gives strictly stronger properties than SwA, when disregarding the difference between SIM-CDP and IND-CDP.

References

1. Abdolmaleki, B., Asadi, A.R., Asadi, V.R., Köpsell, S., Mohee, B., Roustaeifar, N., Zarezadeh, M.: Veridp: Verifiable differentially private training. PoPETS **2026**(3), 48–64 (2026). <https://doi.org/10.56553/POPETS-2026-0070>
2. Addanki, S., Garbe, K., Jaffe, E., Ostrovsky, R., Polychroniadou, A.: Prio+: Privacy preserving aggregate statistics via boolean shares. In: Galdi, C., Jarecki, S. (eds.) SCN'22. pp. 516–539. Springer International Publishing, Cham (2022)

3. Alon, B., Omri, E.: On secure computation of solitary output functionalities with and without broadcast. In: Rothblum, G.N., Wee, H. (eds.) TCC 2023. LNCS, vol. 14370, pp. 94–123. Springer (2023). https://doi.org/10.1007/978-3-031-48618-0_4
4. Balle, B., Barthe, G., Gaboardi, M.: Privacy profiles and amplification by subsampling. *J. Priv. Confidentiality* **10**(1) (2020). <https://doi.org/10.29012/JPC.726>
5. Beimel, A., Lindell, Y., Omri, E., Orlov, I.: $1/p$ -secure multiparty computation without honest majority and the best of both worlds. In: Rogaway, P. (ed.) CRYPTO’11. LNCS, vol. 6841, pp. 277–296. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_16
6. Beimel, A., Nissim, K., Omri, E.: Distributed private data analysis: Simultaneously solving how and what. In: Wagner, D. (ed.) CRYPTO’08. pp. 451–468. Springer Berlin Heidelberg, Berlin, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_25
7. Bell, Z.R., Goldwasser, S., Kim, M.P., Watson, J.L.: Certifying private probabilistic mechanisms. In: Reyzin, L., Stebila, D. (eds.) CRYPTO’24. pp. 348–386. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-68391-6_11
8. Bentov, I., Kumaresan, R.: How to use bitcoin to design fair protocols. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO’14. LNCS, vol. 8617, pp. 421–439. Springer (2014). https://doi.org/10.1007/978-3-662-44381-1_24
9. Biswas, A., Cormode, G.: Interactive proofs for differentially private counting. In: CCS’23. p. 1919–1933. CCS ’23, Association for Computing Machinery, New York, NY, USA (2023). <https://doi.org/10.1145/3576915.3616681>
10. Bitansky, N., Geier, N.: Amplification of non-interactive zero knowledge, revisited. In: Reyzin, L., Stebila, D. (eds.) CRYPTO’24. pp. 361–390. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-68400-5_11
11. Bun, M., Chen, Y.H., Vadhan, S.: Separating computational and statistical differential privacy in the client-server model. In: Hirt, M., Smith, A. (eds.) TCC’16. pp. 607–634. Springer Berlin Heidelberg, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53641-4_23
12. Canetti, R.: Security and composition of multiparty cryptographic protocols. *J. Cryptol.* **13**(1), 143–202 (jan 2000). <https://doi.org/10.1007/s001459910006>, <https://doi.org/10.1007/s001459910006>
13. Canonne, C., Kamath, G., Steinke, T.: The discrete gaussian for differential privacy. *Journal of Privacy and Confidentiality* **12**(1) (Jul 2022). <https://doi.org/10.29012/jpc.784>
14. Champion, J., shelat, a., Ullman, J.: Securely sampling biased coins with applications to differential privacy. In: CCS’19. p. 603–614. CCS ’19, Association for Computing Machinery, New York, NY, USA (2019). <https://doi.org/10.1145/3319535.3354256>, <https://doi.org/10.1145/3319535.3354256>
15. Cleve, R.: Limits on the security of coin flips when half the processors are faulty (extended abstract). In: Hartmanis, J. (ed.) STOC’86. pp. 364–369. ACM (1986). <https://doi.org/10.1145/12130.12168>
16. Cleve, R., Impagliazzo, R.: Martingales, collective coin flipping and discrete control processes. In *other words* **1**, 5 (1993)
17. Corrigan-Gibbs, H., Boneh, D.: Prio: Private, robust, and scalable computation of aggregate statistics. In: 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17). pp. 259–282. USENIX Association, Boston, MA (2017), <https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/corrigan-gibbs>

18. Dong, J., Roth, A., Su, W.J.: Gaussian Differential Privacy. *Journal of the Royal Statistical Society Series B: Statistical Methodology* **84**(1), 3–37 (02 2022). <https://doi.org/10.1111/rssb.12454>, <https://doi.org/10.1111/rssb.12454>
19. Dwork, C.: Differential privacy. In: ICALP’06. p. 1–12. ICALP’06, Springer-Verlag, Berlin, Heidelberg (2006). https://doi.org/10.1007/11787006_1
20. Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., Naor, M.: Our data, ourselves: Privacy via distributed noise generation. In: EUROCRYPT’06. p. 486–503. EUROCRYPT’06, Springer-Verlag, Berlin, Heidelberg (2006). https://doi.org/10.1007/11761679_29
21. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) TCC’06. LNCS, vol. 3876, pp. 265–284. Springer Berlin Heidelberg, Germany, New York, NY, USA (March 4–7, 2006). https://doi.org/10.1007/11681878_14
22. Dwork, C., Roth, A.: The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science* **9**(3–4), 211–407 (2014)
23. Franzese, O., Fang, C., Garg, R., Wang, X., Jha, S., Papernot, N., Dziedzic, A.: Secure noise sampling for differentially private collaborative learning. In: Huang, C., Chen, J., Shieh, S., Lie, D., Cortier, V. (eds.) CCS’25. pp. 4649–4663. ACM (2025). <https://doi.org/10.1145/3719027.3744834>
24. Ghazi, B., Ilango, R., Kamath, P., Kumar, R., Manurangsi, P.: Towards separating computational and statistical differential privacy. In: FOCS’23. pp. 580–599 (2023). <https://doi.org/10.1109/FOCS57990.2023.00042>
25. Ghosh, A., Roughgarden, T., Sundararajan, M.: Universally utility-maximizing privacy mechanisms. *SIAM Journal on Computing* **41**(6), 1673–1693 (2012). <https://doi.org/10.1137/09076828X>
26. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: STOC’87. p. 218–229. STOC ’87, ACM, New York, NY, USA (1987). <https://doi.org/10.1145/28395.28420>
27. Goldreich, O.: *The Foundations of Cryptography - Volume 2: Basic Applications*. Cambridge University Press (2004). <https://doi.org/10.1017/CBO9780511721656>
28. Goldwasser, S., Lindell, Y.: Secure multi-party computation without agreement. *J. Cryptol.* **18**(3), 247–287 (2005). <https://doi.org/10.1007/S00145-005-0319-Z>
29. Gordon, S.D., Katz, J.: Partial fairness in secure two-party computation. In: Gilbert, H. (ed.) EUROCRYPT’10. LNCS, vol. 6110, pp. 157–176. Springer (2010). https://doi.org/10.1007/978-3-642-13190-5_8
30. Gordon, S.D.: On Fairness in Secure Computation. Ph.D. thesis, University of Maryland, College Park, MD, USA (2010), <https://hdl.handle.net/1903/11117>
31. Groce, A., Katz, J., Yerukhimovich, A.: Limits of computational differential privacy in the client/server setting. In: Ishai, Y. (ed.) TCC’11. pp. 417–431. Springer Berlin Heidelberg, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_25
32. Haitner, I., Mazor, N., Shaltiel, R., Silbak, J.: Channels of small log-ratio leakage and characterization of two-party differentially private computation. In: Hofheinz, D., Rosen, A. (eds.) *Theory of Cryptography*. pp. 531–560. Springer International Publishing, Cham (2019)
33. Haitner, I., Mazor, N., Silbak, J., Tsfadia, E.: On the complexity of two-party differential privacy. In: STOC’22. p. 1392–1405. STOC’22, Association for Computing Machinery, New York, NY, USA (2022). <https://doi.org/10.1145/3519935.3519982>
34. Haitner, I., Mazor, N., Silbak, J., Tsfadia, E., Yan, C.: Computationally differentially private inner-product protocols imply oblivious transfer. In: Kalai, Y.T.,

- Kamara, S.F. (eds.) CRYPTO'25. LNCS, vol. 16003, pp. 174–206. Springer (2025). https://doi.org/10.1007/978-3-032-01884-7_6
35. Halevi, S., Ishai, Y., Kushilevitz, E., Makriyannis, N., Rabin, T.: On fully secure MPC with solitary output. In: Hofheinz, D., Rosen, A. (eds.) TCC'19. LNCS, vol. 11891, pp. 312–340. Springer (2019). https://doi.org/10.1007/978-3-030-36030-6_13
 36. Inusah, S., Kozubowski, T.J.: A discrete analogue of the laplace distribution. *Journal of Statistical Planning and Inference* **136**, 1090–1102 (2006)
 37. Keeler, D., Komlo, C., Lepert, E., Veitch, S., He, X.: Dprio: Efficient differential privacy with high utility for prio. *PoPETS* **2023**, 375–390 (07 2023). <https://doi.org/10.56553/popets-2023-0086>
 38. Kii, M., Ichikawa, A., Miura, T.: Lightweight two-party secure sampling protocol for differential privacy. *PoPETS* (2025). <https://doi.org/10.56553/popets-2025-0003>
 39. Lindell, Y.: How to simulate it - A tutorial on the simulation proof technique. In: Lindell, Y. (ed.) *Tutorials on the Foundations of Cryptography*, pp. 277–346. Springer International Publishing (2017). https://doi.org/10.1007/978-3-319-57048-8_6
 40. McGregor, A., Mironov, I., Pitassi, T., Reingold, O., Talwar, K., Vadhan, S.: The limits of two-party differential privacy. In: *FOCS'10*. pp. 81–90 (2010). <https://doi.org/10.1109/FOCS.2010.14>
 41. McGregor, A., Mironov, I., Pitassi, T., Reingold, O., Talwar, K., Vadhan, S.P.: The limits of two-party differential privacy. *ECCC* **TR11-106** (2011), <https://eccc.weizmann.ac.il/report/2011/106>
 42. Meisingseth, F., Rechberger, C.: Sok: Computational and distributed differential privacy for mpc. *PoPETS* **2025**, 420–439 (01 2025). <https://doi.org/10.56553/popets-2025-0023>
 43. Meisingseth, F., Rechberger, C.: Relating definitions of computational differential privacy in wider parameter regimes. *IACR CiC* **2**(4), 7 (2026). <https://doi.org/10.62056/AHEBNJA5>
 44. Meisingseth, F., Rechberger, C., Schmid, F.: Random variable commitments for any sampleable distribution, and a certified laplace mechanism. In: Heninger, N., Rosulek, M. (eds.) CRYPTO'26. LNCS, vol. 16809, pp. 607–639. Springer (2026). https://doi.org/10.1007/978-3-032-35428-0_20
 45. Mironov, I., Pandey, O., Reingold, O., Vadhan, S.: Computational differential privacy. In: Halevi, S. (ed.) CRYPTO'09. pp. 126–142. Springer Berlin Heidelberg, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_8
 46. Moran, T., Naor, M., Segev, G.: An optimally fair coin toss. In: Reingold, O. (ed.) TCC'09. LNCS, vol. 5444, pp. 1–18. Springer (2009). https://doi.org/10.1007/978-3-642-00457-5_1
 47. Pang, Q., Garg, R., Liu, Z., Xiao, H., Smith, V., Zheng, W., Wang, X.: Noisette: Certifying differential privacy mechanisms efficiently. *IACR Cryptol. ePrint Arch.* **2026**, 74 (2026), <https://eprint.iacr.org/2026/074>
 48. Shamsabadi, A.S., Tan, G., Cebere, T., Bellet, A., Haddadi, H., Papernot, N., Wang, X., Weller, A.: Confidential-dpproof: Confidential proof of differentially private training. In: *ICLR'24* (2024), <https://openreview.net/forum?id=PQY2v6VtGe>
 49. Vadhan, S.: *The Complexity of Differential Privacy*, pp. 347–450. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-57048-8_7

50. Wang, C., Su, B., Ye, J., Shokri, R., Su, W.J.: Unified enhancement of privacy bounds for mixture mechanisms via f -differential privacy. In: Oh, A., Naumann, T., Globerson, A., Saenko, K., Hardt, M., Levine, S. (eds.) *NeurIPS'23* (2023), http://papers.nips.cc/paper_files/paper/2023/hash/acb3e20075b0a2dfa3565f06681578e5-Abstract-Conference.html
51. Wasserman, L., Zhou, S.: A statistical framework for differential privacy. *Journal of the American Statistical Association* **105**(489), 375–389 (2010), <http://www.jstor.org/stable/29747034>
52. Wei, C., Yu, R., Fan, Y., Chen, W., Wang, T.: Securely sampling discrete gaussian noise for multi-party differential privacy. In: *CCS'23*. p. 2262–2276. *CCS '23*, ACM, New York, NY, USA (2023). <https://doi.org/10.1145/3576915.3616641>
53. Yao, A.C.: How to generate and exchange secrets (extended abstract). In: *27th Annual Symposium on Foundations of Computer Science*, Toronto, Canada, 27-29 October 1986. pp. 162–167. *IEEE Computer Society* (1986). <https://doi.org/10.1109/SFCS.1986.25>

A Deferred proofs

A.1 Proof of Proposition 1

Proof. For $\mathcal{M}'_A(D)$, note that $\mathcal{M}'_A(D)$ assigns exactly $\Gamma_\perp(\mathcal{M}, D, A)$ more probability mass than $\mathcal{M}(D)$ to $\perp$ but for every $s \in \mathcal{R} : \mathbb{P}(\mathcal{M}'_A(D) = s) \leq \mathbb{P}(\mathcal{M}(D) = s)$. Thus the statistical distance between $\mathcal{M}(D)$ and $\mathcal{M}'_A(D)$ is exactly $\Gamma_\perp(\mathcal{M}, D, A) \leq \Gamma_\perp^{max}(\mathcal{M}, A)$.

For $\mathcal{M}'_{A \neq \perp}$, let μ_D be the measure over $\mathcal{R}$ such that for all $s \in \mathcal{R} : \mu_D(s) = \mathbb{P}(\mathcal{M}'_A(D) = s)$. Note that $\mathcal{M}'(D)$ has exactly $1 - \Gamma_\perp(\mathcal{M}, D, A)$ mass in $\mathcal{R}$ and for every $s \in \mathcal{R} : \mathbb{P}(\mathcal{M}'_A(D) = s) \leq \mathbb{P}(\mathcal{M}(D) = s)$ and $\mathbb{P}(\mathcal{M}'_A(D) = s) \leq \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) = s)$. Thus,

$$\sum_{s \in \mathcal{R}} |\mu_D(s) - \mathbb{P}(\mathcal{M}(D) = s)| = \Gamma_\perp(\mathcal{M}, D, A),$$

and

$$\sum_{s \in \mathcal{R}} |\mu_D(s) - \mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) = s)| = \Gamma_\perp(\mathcal{M}, D, A).$$

Therefore the triangle inequality implies that $\sum_{s \in \mathcal{R}} |\mathbb{P}(\mathcal{M}'_{A \neq \perp}(D) = s) - \mathbb{P}(\mathcal{M}(D) = s)| \leq 2\Gamma_\perp(\mathcal{M}, D, A)$. Hence, by the definition of total variation distance, we have $\mathcal{M}(D) \approx_{\Gamma_\perp(\mathcal{M}, D, A)}^s \mathcal{M}'_{A \neq \perp}(D)$, which implies $\mathcal{M}(D) \approx_{\Gamma_\perp^{max}(\mathcal{M}, A)}^s \mathcal{M}'_{A \neq \perp}(D)$. $\square$

A.2 Proof of Lemma 5

Proof. For any $S \subseteq \mathcal{R}$ and $D \in \mathcal{D}$, we have

$$\begin{aligned} \mathbb{P}(\mathcal{M}_2(D) \in S) &\leq \mathbb{P}(\mathcal{M}_1(D) \in S) + \eta \\ &\leq e^\varepsilon \mathbb{P}(\mathcal{M}_1(D') \in S) + \delta + \eta \\ &\leq e^\varepsilon (\mathbb{P}(\mathcal{M}_2(D') \in S) + \eta) + \delta + \eta \\ &\leq e^\varepsilon \mathbb{P}(\mathcal{M}_2(D') \in S) + \delta + (e^\varepsilon + 1)\eta. \end{aligned}$$

Thus the lemma follows. $\square$

A.3 Proof of Lemma 10

We again note that this proof is simply a translation of a proof in [7] (Section 3.2 of the full version) into our notation.

Proof. Let $S \subseteq \mathcal{R}$ be such $\mathbb{P}(\mathcal{M}(D) \in S) = e^\varepsilon \mathbb{P}(\mathcal{M}(D') \in S) + \delta_{\mathcal{M}}(\varepsilon)$ for some two adjacent $D, D' \in \mathcal{D}$. Note that such a set S exists because $\delta_{\mathcal{M}}$ is the privacy profile of $\mathcal{M}$. Now let A be such that $\Gamma_\perp(D', A) = \gamma_\perp \geq 0$ and $\Gamma_\perp(D, A) = 0$

for all $D \neq D'$. Thus, we have that $\mathbb{P}(\mathcal{M}'_A(D') \in S) = \mathbb{P}(\mathcal{M}(D') \in S) - \gamma_\perp$ and $\mathbb{P}(\mathcal{M}'_A(D) \in S) = \mathbb{P}(\mathcal{M}(D) \in S)$. This implies

$$\begin{aligned}\mathbb{P}(\mathcal{M}'_A(D) \in S) &= \mathbb{P}(\mathcal{M}(D) \in S) = e^\varepsilon \mathbb{P}(\mathcal{M}(D') \in S) + \delta_{\mathcal{M}}(\varepsilon) \\ &= e^\varepsilon (\mathbb{P}(\mathcal{M}'_A(D') \in S) + \gamma_\perp) + \delta_{\mathcal{M}}(\varepsilon) \\ &= e^\varepsilon \mathbb{P}(\mathcal{M}'_A(D') \in S) + \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp.\end{aligned}$$

Therefore $\mathcal{M}'$ is not (ε, δ') -DP for any $\delta' < \delta_{\mathcal{M}}(\varepsilon) + e^\varepsilon \gamma_\perp$. $\square$

A.4 Proof of Lemma 13

Proof. The adversary $\mathcal{S}$ consists of two probabilistic algorithms. First, $\mathcal{S}_1 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run during step two and is given no input. Second, $\mathcal{S}_2 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run in step four, unless $\mathcal{S}_1 = \perp$, and is given s as input. Let $p_1 := \mathbb{P}(\mathcal{S}_1 = \perp)$ and $p_2(s) := \mathbb{P}(\mathcal{S}_2(s) = \perp)$. Then we get

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(D_H) = \perp) = p_1 + (1 - p_1) \cdot \sum_{s \in \mathcal{R}} p_2(s) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s),$$

and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(D_H) = s) = (1 - p_1) \cdot (1 - p_2(s)) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s).$$

Now let $\text{leak} = \{\text{outcome}\}$ in the MoA, which makes $L = (\top, \top, s)$. Let $A_{\text{pre}}(L)$ return s with probability $1 - p_1$, otherwise returning $\perp$. Let $A_{\text{post}}(\perp) = \perp$, $A_{\text{post}}(v) = \mathcal{S}_2(v)$ for all $v \neq \perp$ and define $A := A_{\text{post}} \circ A_{\text{pre}}$. Then we get

$$\mathbb{P}(\mathcal{M}'_A(D_H) = \perp) = p_1 + (1 - p_1) \cdot \sum_{s \in \mathcal{R}} p_2(s) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s),$$

and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\mathcal{M}'_A(D_H) = s) = (1 - p_1) \cdot (1 - p_2(s)) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s).$$

$\square$

A.5 Proof of Lemma 14

Proof. The adversary $\mathcal{S}$ consists of only one probabilistic algorithm $\mathcal{S}_1$. This $\mathcal{S}_1 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run in step two and is given input $\bar{D}_C$. Let $p_1(\bar{D}_C) := \mathbb{P}(\mathcal{S}_1(\bar{D}_C) = \perp)$. Then we get $\mathbb{P}(\text{Out}^{\mathcal{S}}(\bar{D}) = \perp) = p_1(\bar{D}_C)$, and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(\bar{D}) = s) = (1 - p_1(\bar{D}_C)) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s).$$

Now let $\text{leak} = \{\text{DB}\}$ in the MoA, which makes $L = (\bar{D}, \top, \top)$. Let $A(L)$ return $\top$ with probability $1 - p_1(\bar{D}_C)$, otherwise returning $\perp$. Then we get $\mathbb{P}(\mathcal{M}'_A(\bar{D}) = \perp) = p_1(\bar{D}_C)$, and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\mathcal{M}'_A(\bar{D}) = s) = (1 - p_1(\bar{D}_C)) \cdot \mathbb{P}(\mathcal{M}(\bar{D}) = s).$$

$\square$

A.6 Proof of Lemma 15

Proof. The adversary $\mathcal{S}$ consists of only one probabilistic algorithm. This $\mathcal{S}_1 : \{0, 1\}^* \rightarrow \{\top, \perp\}$ is run during step two and is given no input. Let $p_1 := \mathbb{P}(\mathcal{S}_1 = \perp)$. Then we get $\mathbb{P}(\text{Out}^{\mathcal{S}}(D_H) = \perp) = p_1$, and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\text{Out}^{\mathcal{S}}(D_H) = s) = (1 - p_1) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s).$$

Now let $\text{leak} = \{\}$ in the MoA, which makes $L = (\top, \top, \top)$. Let $A(L)$ return $\top$ with probability $1 - p_1$, otherwise returning $\perp$. Then we get $\mathbb{P}(\mathcal{M}'_A(D_H) = \perp) = p_1$, and for all $s \in \mathcal{R}$,

$$\mathbb{P}(\mathcal{M}'_A(D_H) = s) = (1 - p_1) \cdot \mathbb{P}(\mathcal{M}_{\bar{D}_C}(D_H) = s).$$

□