APPENDIX

In the main text, we used the fact that we could bound the amount of privacy budget ϵ'_{leaf} needed to label leaves with expected worst-case incurred error at most $\mathcal{E}_{max}$. By limiting the amount of privacy budget for leaf labeling this way we make sure to leave more privacy budget for node selection when possible. We give a short proof of the theorem below.

Corollary 4. *For K classes, n samples and depth d trees, the amount of privacy budget ϵ'_{leaf} needed for labeling leaves with the permute-and-flip mechanism with expected error $\mathbb{E}[\mathcal{E}(\mathcal{M}_{PF}, \vec{N})]$ of at most $\mathcal{E}_{max}$ is:*

$$\epsilon'_{\text{leaf}} \leq \frac{2^d \max_p 2\log(\frac{1}{p})\left(1 - \frac{1-(1-p)^K}{Kp}\right)}{n\,\mathcal{E}_{max}} \ ,$$

Proof. Recall Proposition 4 from the permute-and-flip paper [26] that for a vector of candidates with errors $\vec{q} \in \mathbb{R}^K$ the expected worst case error $\mathbb{E}[\mathcal{E}(\mathcal{M}_{PF}, \vec{q})]$ occurs when all but one candidates share the same error c (and thus share probability of being selected $p = \exp(\frac{\epsilon}{2\Delta}c)$). The expected errors for such vectors of this form are:

$$\mathbb{E}[\mathcal{E}(\mathcal{M}_{PF}, \vec{q})] = \frac{2\Delta}{\epsilon}\log\left(\frac{1}{p}\right)\left(1 - \frac{1-(1-p)^K}{Kp}\right) \ .$$

The worst-case expected error can be found by maximizing over $p \in [0, 1]$, i.e. after substituting sensitivity Δ=1 and ϵ=ϵ'_{leaf}:

$$\max_p \frac{2}{\epsilon'_{\text{leaf}}}\log\left(\frac{1}{p}\right)\left(1 - \frac{1-(1-p)^K}{Kp}\right) \ .$$

Now we do not want to bound the total error but the percentage error so we divide by n samples, and since we can incur error for every leaf we multiply by 2^d. After bounding by the user-specified value $\mathcal{E}_{max}$ we find a sufficient value for ϵ'_{leaf}:

$$\frac{2^d \max_p \frac{2}{\epsilon'_{\text{leaf}}}\log(\frac{1}{p})\left(1 - \frac{1-(1-p)^K}{Kp}\right)}{n} \leq \mathcal{E}_{max} \ ,$$

$$\frac{2^d \max_p 2\log(\frac{1}{p})\left(1 - \frac{1-(1-p)^K}{Kp}\right)}{n\,\mathcal{E}_{max}} \leq \epsilon'_{\text{leaf}} \ . \qquad \square$$

In our implementation, we solve the maximization term numerically using Scipy.

We summarize the properties of the datasets that we included in our benchmark in Table IV, dataset sizes are displayed after removing rows with missing values. Since UCI datasets are imbalanced, private models often perform worse than guessing the majority class for low privacy budgets.

We measured the runtime of all methods when performing 5-fold cross validations and display the results in Table V. Regular decision trees run in milliseconds benefitting from the fast implementation by Scikit-learn [57]. DiffPrivLib does not need to perform node selection operations and thus only spends milliseconds on propagating data points to the leaves and labeling them. DPGDF, BDPT and PrivaTree usually run in seconds, however, on large numerical datasets BDPT takes minutes.

In the main text we displayed results for depth 4 trees with a privacy budget of $\epsilon = 0.1$. Although this is generally considered as a good value for privacy, we also display results for $\epsilon = 0.01$ and $\epsilon = 1$ in Tables VI and VII respectively.

In the main text, we showed a comparison between the poisoning robustness guarantees of PrivaTree and private logistic regression on numerical datasets. In Table VIII we show results on data with categorical features encoded as integers.

TABLE IV: Properties of the datasets used in this work. Rows with missing values were removed. UCI datasets are often imbalanced.

Dataset	**Samples**	**Features**	**Categorical features**	**Majority class share**
		Numerical data		
Bioresponse	3,434	419	0	0.500
Diabetes130US	71,090	7	0	0.500
Higgs	940,160	24	0	0.500
MagicTelescope	13,376	10	0	0.500
MiniBooNE	72,998	50	0	0.500
bank-marketing	10,578	7	0	0.500
california	20,634	8	0	0.500
covertype	566,602	10	0	0.500
credit	16,714	10	0	0.500
default-of-credit-card-clients	13,272	20	0	0.500
electricity	38,474	7	0	0.500
eye_movements	7,608	20	0	0.500
heloc	10,000	22	0	0.500
house_16H	13,488	16	0	0.500
jannis	57,580	54	0	0.500
pol	10,082	26	0	0.500
		Numerical & categorical data		
albert	58,252	31	10	0.500
compas-two-years	4,966	11	8	0.500
covertype	423,680	54	44	0.500
default-of-credit-card-clients	13,272	21	1	0.500
electricity	38,474	8	1	0.500
eye_movements	7,608	23	3	0.500
road-safety	111,762	32	3	0.500
		UCI datasets (numerical & categorical)		
adult	45,222	14	8	0.752
breast-w	683	9	0	0.650
diabetes	768	8	0	0.651
mushroom	5,644	22	22	0.618
nursery	12,960	8	8	0.667
vote	232	16	16	0.534

TABLE V: Mean runtimes in seconds and standard errors at ϵ=0.1 for trees of depth 4 with 5 repetitions.

OpenML dataset	**decision tree**	**BDPT**	**PrivaTree***	**DPGDF**	**DiffPrivLib**	**PrivaTree**
	no privacy	leaking numerical splits		differential privacy		
Numerical data						
Bioresponse	<1 ± 0	2 ± 0	1 ± 0	-	<1 ± 0	1 ± 0
Diabetes130US	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
Higgs	9 ± 0	-	2 ± 0	-	6 ± 0	1 ± 0
MagicTelescope	<1 ± 0	2 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
MiniBooNE	2 ± 0	366 ± 15	<1 ± 0	-	1 ± 0	<1 ± 0
bank-marketing	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
california	<1 ± 0	1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
covertype	1 ± 0	9 ± 0	1 ± 0	-	4 ± 0	<1 ± 0
credit	<1 ± 0	1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
default-of-credit-card-clients	<1 ± 0	1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
electricity	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
eye_movements	<1 ± 0	1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
heloc	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
house_16H	<1 ± 0	2 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
jannis	1 ± 0	173 ± 14	<1 ± 0	-	1 ± 0	<1 ± 0
pol	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
Numerical & categorical data						
albert	<1 ± 0	2 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
compas-two-years	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
covertype	2 ± 0	17 ± 1	1 ± 0	1 ± 0	4 ± 0	1 ± 0
default-of-credit-card-clients	<1 ± 0	1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
electricity	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
eye_movements	<1 ± 0	1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
road-safety	1 ± 0	54 ± 0	<1 ± 0	<1 ± 0	1 ± 0	<1 ± 0
UCI datasets (numerical & categorical)						
adult	<1 ± 0	1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
breast-w	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
diabetes	<1 ± 0	<1 ± 0	<1 ± 0	-	<1 ± 0	<1 ± 0
mushroom	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
nursery	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0
vote	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0	<1 ± 0

TABLE VI: 5-fold cross-validated mean test accuracy scores and standard errors at ϵ=0.01 for trees of depth 4. PrivaTree* uses non-private quantiles, DPGDF only ran on categorical features.

OpenML dataset	**decision tree** no privacy	**BDPT** leaking numerical splits	**PrivaTree*** leaking numerical splits	**DPGDF** differential privacy	**DiffPrivLib** differential privacy	**PrivaTree** differential privacy
Numerical data						
Bioresponse	.711 ± .006	.500 ± .001	**.524** ± .012	-	**.509** ± .009	.501 ± .005
Diabetes130US	.606 ± .001	.509 ± .008	**.554** ± .008	-	.521 ± .017	**.527** ± .008
Higgs	.657 ± .001	timeout	**.583** ± .021	-	.509 ± .004	**.565** ± .016
MagicTelescope	.781 ± .006	.500 ± .000	**.624** ± .038	-	.562 ± .033	**.594** ± .033
MiniBooNE	.871 ± .001	.500 ± .000	**.721** ± .009	-	**.512** ± .010	.502 ± .001
bank-marketing	.771 ± .005	.500 ± .001	**.556** ± .010	-	**.556** ± .032	.539 ± .040
california	.783 ± .002	.500 ± .000	**.566** ± .023	-	**.546** ± .010	.530 ± .017
covertype	.740 ± .001	.501 ± .001	**.698** ± .016	-	.535 ± .007	**.724** ± .003
credit	.748 ± .001	.498 ± .002	**.630** ± .027	-	**.507** ± .009	.504 ± .002
default-of-credit.	.704 ± .002	.500 ± .000	**.571** ± .012	-	**.544** ± .034	.531 ± .028
electricity	.734 ± .002	.500 ± .000	**.608** ± .008	-	.549 ± .020	**.561** ± .023
eye_movements	.574 ± .003	.500 ± .000	**.503** ± .005	-	.512 ± .005	**.520** ± .013
heloc	.704 ± .004	.487 ± .008	**.602** ± .012	-	.526 ± .017	**.550** ± .028
house_16H	.815 ± .004	.500 ± .000	**.657** ± .038	-	.562 ± .021	**.578** ± .018
jannis	.715 ± .002	.500 ± .000	**.570** ± .022	-	**.578** ± .020	.574 ± .017
pol	.929 ± .003	.501 ± .001	**.575** ± .026	-	**.547** ± .025	.537 ± .026
Numerical & categorical data						
albert	.640 ± .002	.500 ± .000	**.541** ± .012	.505 ± .002	**.517** ± .007	.509 ± .004
compas-two-years	.672 ± .006	.538 ± .008	**.588** ± .017	.505 ± .013	**.557** ± .014	.529 ± .011
covertype	.756 ± .000	.501 ± .001	**.739** ± .003	.515 ± .009	.540 ± .012	**.735** ± .001
default-of-credit.	.707 ± .004	.500 ± .000	**.543** ± .014	.498 ± .014	**.535** ± .020	.525 ± .019
electricity	.732 ± .002	.500 ± .000	**.615** ± .028	.510 ± .001	.562 ± .017	**.588** ± .020
eye_movements	.579 ± .001	.500 ± .000	**.511** ± .007	.496 ± .007	**.510** ± .007	.498 ± .002
road-safety	.728 ± .001	.500 ± .000	**.522** ± .005	**.685** ± .001	.554 ± .027	.512 ± .005
UCI datasets (numerical & categorical)						
adult	.840 ± .001	**.752** ± .000	.750 ± .003	.744 ± .007	**.752** ± .000	.751 ± .001
breast-w	.950 ± .007	.517 ± .066	**.757** ± .048	-	**.846** ± .032	.673 ± .086
diabetes	.734 ± .006	**.612** ± .036	.547 ± .051	-	**.608** ± .038	.566 ± .055
mushroom	.971 ± .001	.576 ± .062	**.770** ± .044	.546 ± .083	**.716** ± .052	.694 ± .059
nursery	1.000 ± .000	.535 ± .024	**.731** ± .047	.620 ± .078	.654 ± .008	**.685** ± .050
vote	.944 ± .013	**.721** ± .065	.624 ± .068	.496 ± .119	.612 ± .035	**.689** ± .082

TABLE VII: 5-fold cross-validated mean test accuracy scores and standard errors at ϵ=1 for trees of depth 4. PrivaTree* uses non-private quantiles, DPGDF only ran on categorical features.

OpenML dataset	**decision tree**	**BDPT**	**PrivaTree***	**DPGDF**	**DiffPrivLib**	**PrivaTree**
	no privacy	leaking numerical splits		differential privacy		
Numerical data						
Bioresponse	.711 ± .006	.505 ± .005	**.557** ± .006	-	.518 ± .007	**.576** ± .024
Diabetes130US	.606 ± .001	.544 ± .002	**.599** ± .002	-	.531 ± .007	**.559** ± .001
Higgs	.657 ± .001	timeout	**.659** ± .000	-	.504 ± .002	**.601** ± .002
MagicTelescope	.781 ± .006	.500 ± .000	**.753** ± .004	-	.665 ± .039	**.755** ± .006
MiniBooNE	.871 ± .001	.601 ± .004	**.863** ± .002	-	.505 ± .003	**.765**± .012
bank-marketing	.771 ± .005	.599 ± .004	**.745** ± .002	-	.523 ± .009	**.742** ± .003
california	.783 ± .002	.500 ± .000	**.765** ± .002	-	.547 ± .011	**.758** ± .004
covertype	.740 ± .001	.529 ± .001	**.745** ± .003	-	.527 ± .006	**.729** ± .001
credit	.748 ± .001	.512 ± .012	**.743** ± .005	-	.513 ± .005	**.581** ± .007
default-of-credit.	.704 ± .002	.526 ± .016	**.685** ± .002	-	.557 ± .021	**.688** ± .002
electricity	.734 ± .002	.609 ± .002	**.738** ± .003	-	.532 ± .015	**.635** ± .002
eye_movements	.574 ± .003	.500 ± .000	**.533** ± .007	-	**.511** ± .006	.506 ± .005
heloc	.704 ± .004	.650 ± .011	**.694** ± .003	-	.575 ± .027	**.695** ± .003
house_16H	.815 ± .004	.708 ± .010	**.788** ± .010	-	.567 ± .019	**.708** ± .006
jannis	.715 ± .002	.579 ± .032	**.704** ± .002	-	.531 ± .007	**.701** ± .004
pol	.929 ± .003	.653 ± .024	**.904** ± .004	-	.572 ± .019	**.883** ± .007
Numerical & categorical data						
albert	.640 ± .002	.632 ± .002	**.634** ± .002	.505 ± .002	.510 ± .003	**.593** ± .005
compas-two-years	.672 ± .006	.633 ± .008	**.650** ± .011	.584 ± .011	.574 ± .004	**.606** ± .010
covertype	.756 ± .000	.613 ± .001	**.756** ± .001	.547 ± .008	.512 ± .005	**.755** ± .002
default-of-credit.	.707 ± .004	.500 ± .000	**.689** ± .003	.528 ± .005	.531 ± .014	**.692** ± .003
electricity	.732 ± .002	.608 ± .004	**.738** ± .003	.521 ± .004	.573 ± .016	**.642** ± .006
eye_movements	.579 ± .001	.499 ± .002	**.507** ± .010	**.531** ± .004	.530 ± .009	.528 ± .009
road-safety	.728 ± .001	.460 ± .001	**.711** ± .002	.629 ± .024	.510 ± .002	**.712** ± .003
UCI datasets (numerical & categorical)						
adult	.840 ± .001	.811 ± .003	**.820** ± .001	.754 ± .001	.756 ± .003	**.822** ± .002
breast-w	.950 ± .007	.641 ± .009	**.927** ± .011	-	**.950** ± .008	.939 ± .007
diabetes	.734 ± .006	.646 ± .008	**.664** ± .007	-	.655 ± .002	**.681** ± .009
mushroom	.971 ± .001	.956 ± .004	**.959** ± .008	.695 ± .024	.740 ± .049	**.949** ± .005
nursery	1.000 ± .000	**1.000** ± .000	**1.000** ± .000	.664 ± .003	.789 ± .057	**1.000** ± .000
vote	.944 ± .013	.862 ± .032	**.871** ± .032	**.875** ± .016	**.875** ± .030	.867 ± .057

TABLE VIII: 5-fold cross-validated mean test accuracy and poisoning accuracy guarantee against a percentage of poisoned samples on mixed numerical/categorical datasets. Stronger privacy provides stronger poisoning robustness but comes at the cost of clean dataset accuracy. Since *vote* and *diabetes* do not have enough samples, we do not the compute 0.1% guarantee.

dataset	**method**	ϵ	**accuracy**	**0.1% guarantee**	**0.5% guarantee**	**1% guarantee**
		Numerical & categorical data				
albert	PrivaTree	.01	.50	.32	.05	.01
		.1	.51	.01	-	-
	DiffPrivLib LR	.01	**.52**	**.33**	**.05**	**.01**
		.1	**.52**	.01	-	-
compas-two-years	PrivaTree	.01	.50	**.49**	**.42**	**.34**
		.1	**.58**	.43	.09	.01
	DiffPrivLib LR	.01	.47	.45	.39	.32
		.1	.47	.35	.07	.01
covertype	PrivaTree	.01	**.74**	**.03**	-	-
		.1	**.74**	-	-	-
	DiffPrivLib LR	.01	.55	.02	-	-
		.1	.63	-	-	-
default-of-credit-card-clients	PrivaTree	.01	**.58**	**.52**	**.34**	**.20**
		.1	.55	.20	-	-
	DiffPrivLib LR	.01	.50	.45	.29	.17
		.1	.49	.18	-	-
electricity	PrivaTree	.01	.53	**.39**	**.12**	**.03**
		.1	**.61**	.03	-	-
	DiffPrivLib LR	.01	.52	.39	.11	.02
		.1	.57	.03	-	-
eye_movements	PrivaTree	.01	.50	**.47**	**.37**	**.27**
		.1	**.51**	.28	.03	-
	DiffPrivLib LR	.01	.50	**.47**	**.37**	**.27**
		.1	**.51**	.28	.03	-
road-safety	PrivaTree	.01	.54	**.22**	**.01**	-
		.1	**.69**	-	-	-
	DiffPrivLib LR	.01	.51	.21	.01	-
		.1	.56	-	-	-
		UCI datasets (numerical & categorical)				
adult	PrivaTree	.01	.75	**.52**	**.12**	**.02**
		.1	**.79**	.02	-	-
	DiffPrivLib LR	.01	.54	.38	.09	.02
		.1	.76	.02	-	-
breast-w	PrivaTree	.01	.67	-	.66	**.64**
		.1	**.87**	-	**.72**	.53
	DiffPrivLib LR	.01	.42	-	.41	.40
		.1	.78	-	.64	.47
diabetes	PrivaTree	.01	.55	-	.53	.52
		.1	**.64**	-	.48	.35
	DiffPrivLib LR	.01	.58	-	**.56**	**.55**
		.1	.42	-	.31	.23
mushroom	PrivaTree	.01	.72	**.69**	**.58**	**.46**
		.1	**.78**	.52	.09	.01
	DiffPrivLib LR	.01	.49	.47	.39	.31
		.1	.60	.40	.07	.01
nursery	PrivaTree	.01	.71	**.64**	**.42**	**.25**
		.1	**1.00**	.37	.01	-
	DiffPrivLib LR	.01	.55	.50	.33	.20
		.1	.95	.35	.01	-
vote	PrivaTree	.01	.57	-	-	.57
		.1	.57	-	-	.52
	DiffPrivLib LR	.01	**.60**	-	-	**.59**
		.1	.46	-	-	.42