



ppAURORA: Privacy Preserving Area Under Receiver Operating Characteristic and Precision-Recall Curves

Ali Burak Ünal, Nico Pfeifer, Mete Akgün

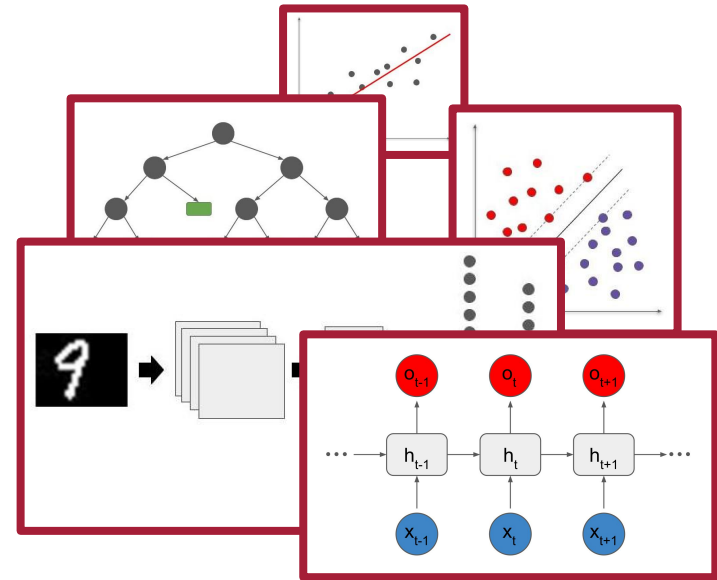
Motivation

- Data is everywhere!



Motivation

- Data is everywhere!
- Machine learning algorithms demand data.



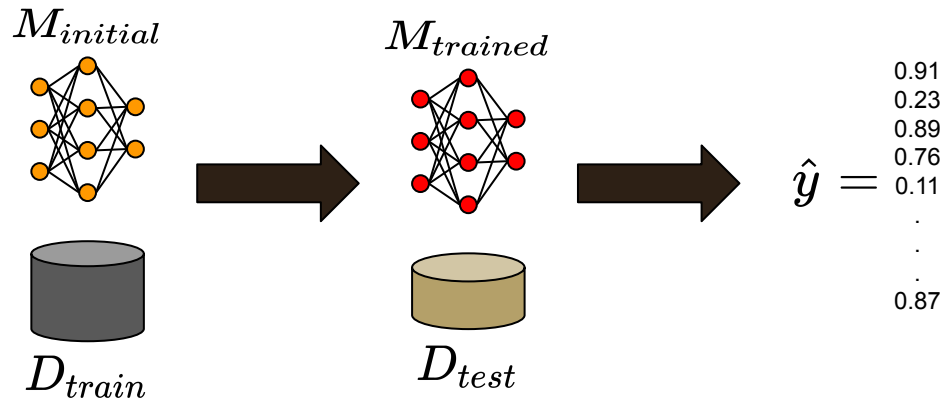
Motivation

- Data is everywhere!
- Machine learning algorithms demand data.
- Privacy of the sensitive information!



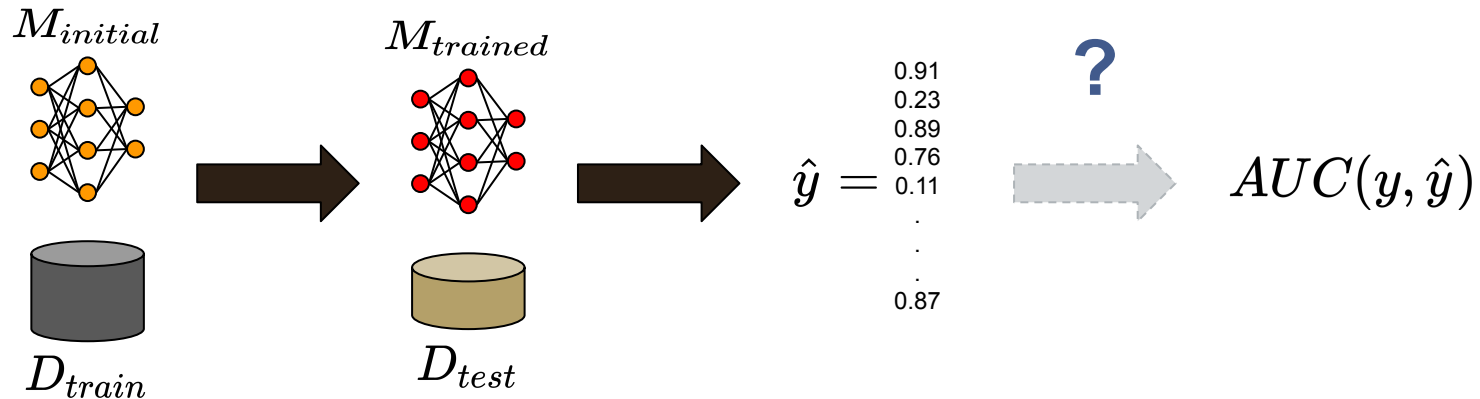
Motivation

- Data is everywhere!
- Machine learning algorithms demand data.
- Privacy of the sensitive information!
 - Privacy preserving model training and testing



Motivation

- Data is everywhere!
- Machine learning algorithms demand data.
- Privacy of the sensitive information!
 - Privacy preserving model training and testing
 - How about the privacy preserving model evaluation such as the area under curve?



ppAURORA

- Privacy preserving model evaluation based on 3-party computation (MPC) framework^[1]

[1] Ünal, Ali Burak, Nico Pfeifer, and Mete Akgün. "CECILIA: Comprehensive secure machine learning framework." arXiv preprint arXiv:2202.03023 (2022).



ppAURORA

- Privacy preserving model evaluation based on 3-party computation (MPC) framework^[1]

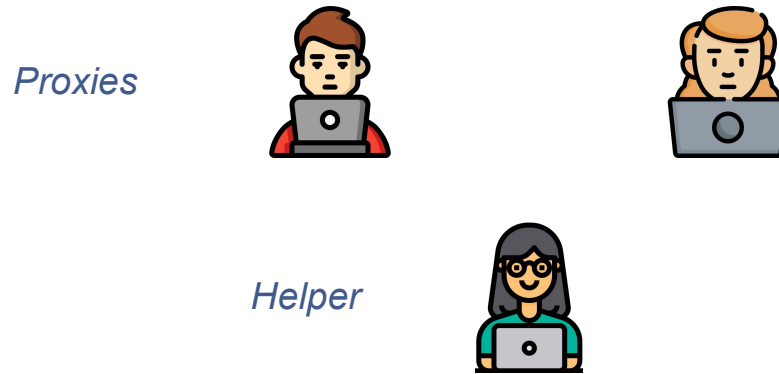
Proxies



[1] Ünal, Ali Burak, Nico Pfeifer, and Mete Akgün. "CECILIA: Comprehensive secure machine learning framework." arXiv preprint arXiv:2202.03023 (2022).

ppAURORA

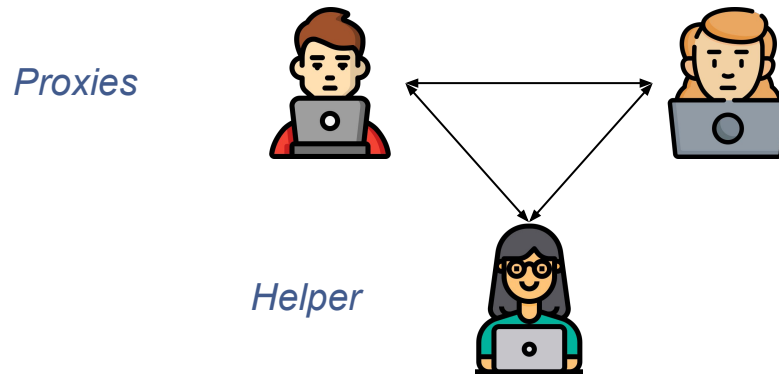
- Privacy preserving model evaluation based on 3-party computation (MPC) framework^[1]



[1] Ünal, Ali Burak, Nico Pfeifer, and Mete Akgün. "CECILIA: Comprehensive secure machine learning framework." arXiv preprint arXiv:2202.03023 (2022).

ppAURORA

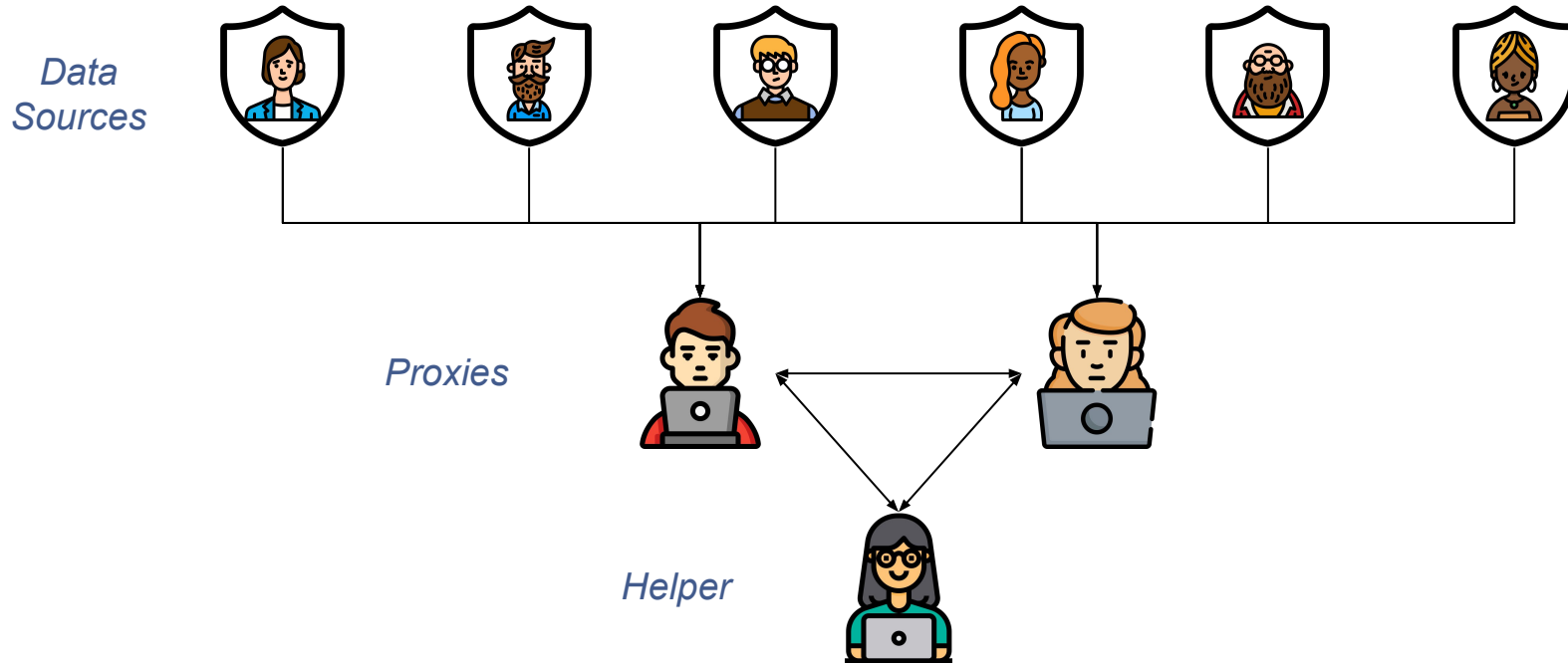
- Privacy preserving model evaluation based on 3-party computation (MPC) framework^[1]



[1] Ünal, Ali Burak, Nico Pfeifer, and Mete Akgün. "CECILIA: Comprehensive secure machine learning framework." arXiv preprint arXiv:2202.03023 (2022).

ppAURORA

- Privacy preserving model evaluation based on 3-party computation (MPC) framework^[1]



[1] Ünal, Ali Burak, Nico Pfeifer, and Mete Akgün. "CECILIA: Comprehensive secure machine learning framework." arXiv preprint arXiv:2202.03023 (2022).

ppAURORA

- Privacy preserving model evaluation based on 3-party computation (MPC) framework
- Area under the curve (AUC) as the model evaluation metric
 - Summarizes the plot-based model evaluation metrics by measuring the area between the curve and the x-axis
 - Receiver operating characteristic (ROC) curve
 - Precision-Recall (PR) Curve

ppAURORA

- Privacy preserving model evaluation based on 3-party computation (MPC) framework
- Area under the curve (AUC) as the model evaluation metric
 - Summarizes the plot-based model evaluation metrics by measuring the area between the curve and the x-axis
 - Receiver operating characteristic (ROC) curve
 - Precision-Recall (PR) Curve
- Exact AUC computation via the MPC building blocks
 - Especially for the small size test set

Area Under the ROC Curve (AUROC)

- ppAURORA for the area under the ROC curve (AUROC)



Area Under the ROC Curve (AUROC)

- ppAURORA for the area under the ROC curve (AUROC)
- Two versions
 - No tie condition in the prediction scores (AUROC no-tie)
 - With tie condition in the prediction scores (AUROC with-tie)

Area Under the ROC Curve (AUROC)

- For AUROC no-tie

$$AUROC = \frac{\sum_{i=1}^M (TP[i] \cdot (FP[i] - FP[i-1]))}{T \cdot F}$$



Area Under the ROC Curve (AUROC)

- For AUROC no-tie

$$AUROC = \frac{\sum_{i=1}^M \left(TP[i] \cdot (FP[i] - FP[i-1]) \right)}{T \cdot F}$$

Diagram illustrating the AUROC formula with annotations:

- $\sum_{i=1}^M$: all samples
- $TP[i]$: # true positives
- $FP[i] - FP[i-1]$: # false positives
- $T \cdot F$: # true samples (T) and # false samples (F)

Area Under the ROC Curve (AUROC)

- For AUROC no-tie

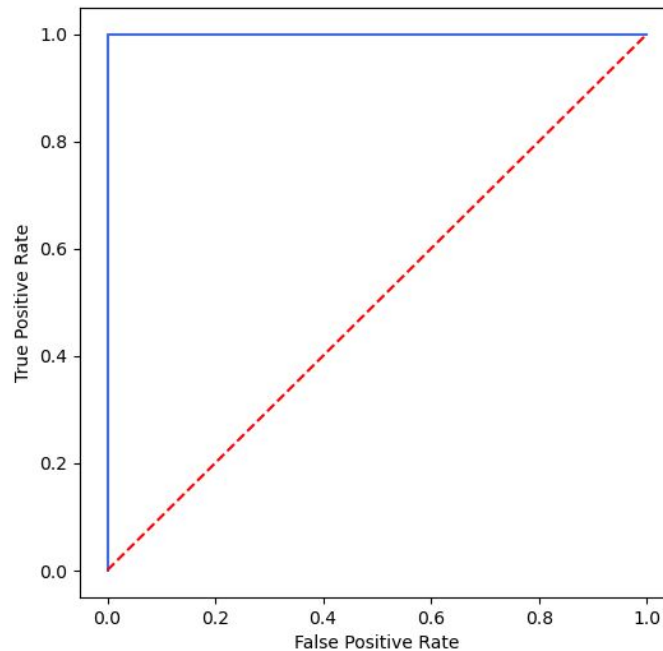
$$AUROC = \frac{\sum_{i=1}^M (TP[i] \cdot (FP[i] - FP[i-1]))}{T \cdot F}$$

The diagram illustrates the components of the AUROC formula with annotations:

- all samples**: Points to the summation index i .
- # true positives**: Points to $TP[i]$.
- # false positives**: Points to $FP[i] - FP[i-1]$.
- MUL**: A red label with arrows pointing to the multiplication operation \cdot in the numerator and the denominator $T \cdot F$.
- DIV**: A red label with an arrow pointing to the division operation $\frac{\dots}{\dots}$.
- # true samples**: Points to T in the denominator.
- # false samples**: Points to F in the denominator.

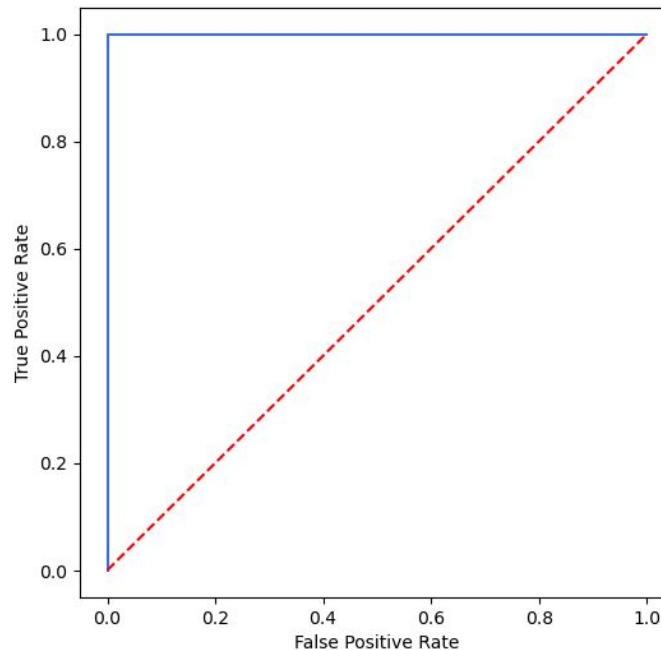
Why AUROC *with-tie*?

Prediction Score	Label
0.5	1
0.5	1
0.5	1
0.5	1
0.5	1
0.5	0
0.5	0
0.5	0
0.5	0
0.5	0



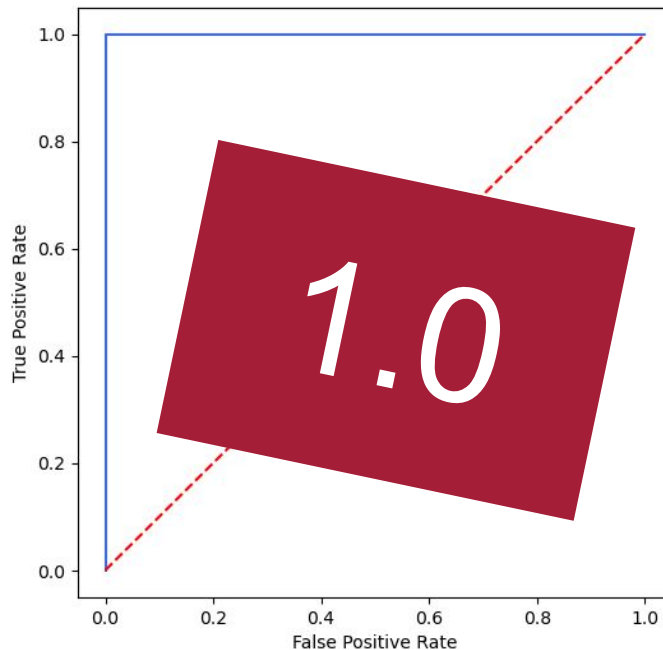
Why AUROC *with-tie*?

TPR	FPR	Prediction Score	Label
0.2	0	0.5	1
0.4	0	0.5	1
0.6	0	0.5	1
0.8	0	0.5	1
1	0	0.5	1
1	0.2	0.5	0
1	0.4	0.5	0
1	0.6	0.5	0
1	0.8	0.5	0
1	1	0.5	0



Why AUROC *with-tie*?

TPR	FPR	Prediction Score	Label
0.2	0	0.5	1
0.4	0	0.5	1
0.6	0	0.5	1
0.8	0	0.5	1
1	0	0.5	1
1	0.2	0.5	0
1	0.4	0.5	0
1	0.6	0.5	0
1	0.8	0.5	0
1	1	0.5	0



Area Under the ROC Curve (AUROC)

- For AUROC no-tie

$$AUROC = \frac{\sum_{i=1}^M (TP[i] \cdot (FP[i] - FP[i-1]))}{T \cdot F}$$

Diagram annotations for the AUROC no-tie formula:

- all samples: points to the summation index i
- # true positives: points to $TP[i]$
- # false positives: points to $FP[i] - FP[i-1]$
- # true samples: points to T
- # false samples: points to F

- For AUROC with-tie

$$AUROC = \sum_{i=1}^{\Theta} \left(\frac{(TP[i] + TP[i-1]) \cdot (FP[i] - FP[i-1])}{2 \cdot T \cdot F} \right)$$

Area Under the ROC Curve (AUROC)

- For AUROC no-tie

$$AUROC = \frac{\sum_{i=1}^M (TP[i] \cdot (FP[i] - FP[i-1]))}{T \cdot F}$$

Diagram annotations for the AUROC no-tie formula:

- $\sum_{i=1}^M$: all samples
- $TP[i]$: # true positives
- $FP[i] - FP[i-1]$: # false positives
- $T \cdot F$: # true samples (T) and # false samples (F)

- For AUROC with-tie

threshold samples
determined via secure tie detection

$$AUROC = \sum_{i=1}^{\Theta} \left(\frac{(TP[i] + TP[i-1]) \cdot (FP[i] - FP[i-1])}{2 \cdot T \cdot F} \right)$$

Area Under the ROC Curve (AUROC)

- For AUROC no-tie

$$AUROC = \frac{\sum_{i=1}^M (TP[i] \cdot (FP[i] - FP[i-1]))}{T \cdot F}$$

all samples \rightarrow $\sum_{i=1}^M$
 # true positives \rightarrow $TP[i]$
 # false positives \rightarrow $(FP[i] - FP[i-1])$
 $T \cdot F$
 # true samples \rightarrow T
 # false samples \rightarrow F

- For AUROC with-tie

$$AUROC = \sum_{i=1}^{\Theta} \left(\frac{(TP[i] + TP[i-1]) \cdot (FP[i] - FP[i-1])}{2 \cdot T \cdot F} \right)$$

threshold samples determined via secure tie detection \rightarrow $\sum_{i=1}^{\Theta}$
 MUL \rightarrow $(TP[i] + TP[i-1]) \cdot (FP[i] - FP[i-1])$
 DIV \rightarrow $2 \cdot T \cdot F$

Area Under the Precision-Recall Curve (AUPR)

- ppAURORA for the area under the PR curve (AUPR)



Area Under the Precision-Recall Curve (AUPR)

- ppAURORA for the area under the PR curve (AUPR)
- Similar to AUROC with-tie
 - Precision and recall can change at the same time.
 - No common denominator though

Area Under the Precision-Recall Curve (AUPR)

- ppAURORA for the area under the PR curve (AUPR)
- Similar to AUROC with-tie
 - Precision and recall can change at the same time.
 - No common denominator though

$$AUROC = \sum_{i=1}^{\Theta} \left(\underset{\substack{\uparrow \\ \text{Precision}}}{PRE[i-1]} \cdot \underset{\substack{\uparrow \\ \text{Recall}}}{(REC[i] - REC[i-1])} + \frac{(PRE[i] - PRE[i-1]) \cdot (REC[i] - REC[i-1])}{2} \right)$$

Area Under the Precision-Recall Curve (AUPR)

- ppAURORA for the area under the PR curve (AUPR)
- Similar to AUROC with-tie
 - Precision and recall can change at the same time.
 - No common denominator though

$$AUROC = \sum_{i=1}^{\Theta} \left(\underbrace{PRE[i-1]}_{\text{Precision}} \cdot \underbrace{(REC[i] - REC[i-1])}_{\text{Recall}} + \frac{\underbrace{(PRE[i] - PRE[i-1])}_{\text{Precision}} \cdot \underbrace{(REC[i] - REC[i-1])}_{\text{Recall}}}{2} \right)$$

The diagram illustrates the components of the AUROC formula. Blue arrows point from the labels 'Precision' and 'Recall' to the corresponding terms in the equation. Red arrows and labels 'DIV' and 'MUL' indicate the operations: 'DIV' points to the division symbol in the second term, and 'MUL' points to the multiplication symbols in both terms.

Sorting

- The first task to perform before both AUROC and AUPR
 - Individually sorted lists from multiple data sources
- Merging individually sorted lists using the MPC building blocks
 - Parametric sorting algorithm adjusting the privacy-performance trade-off
- Skipping due to the time limitation

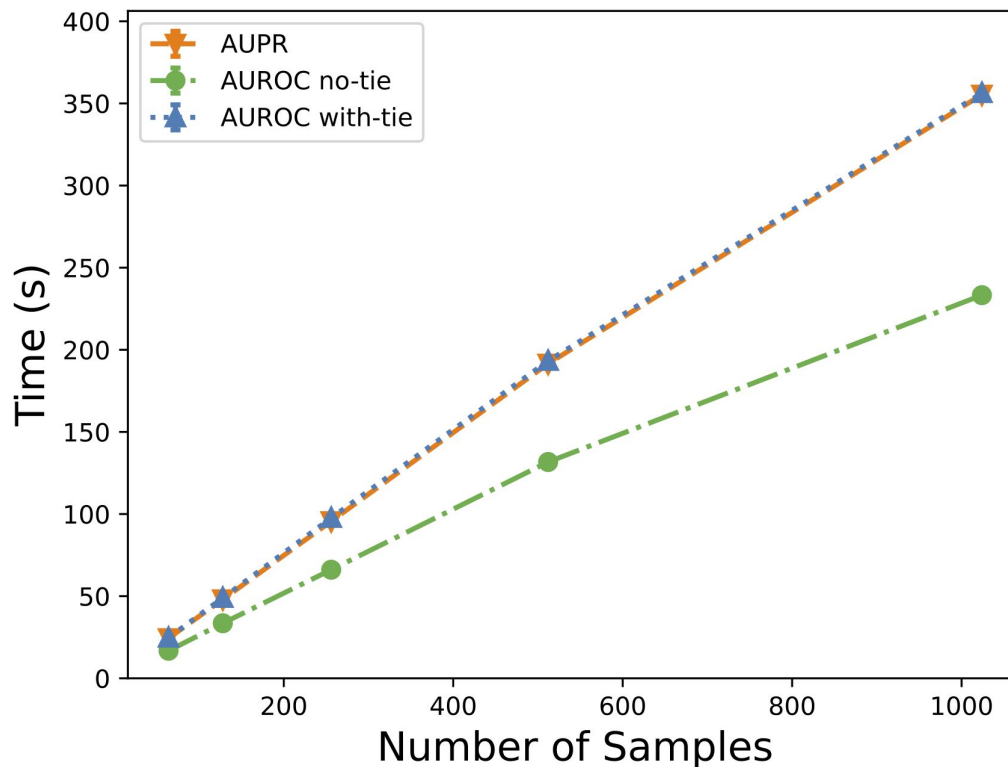


Results

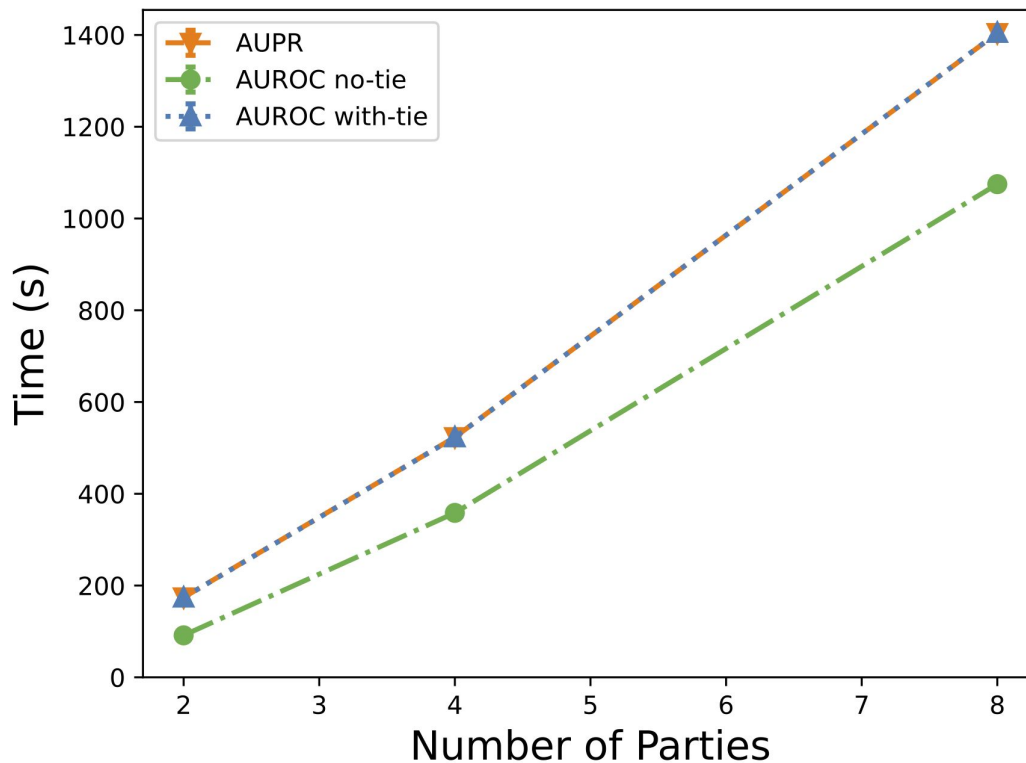
- Correctness analysis on
 - Acute Myeloid Leukemia dataset
 - UCI Heart Disease dataset
 - Same as the result of the plaintext analysis

- Scalability analysis on
 - Synthetic dataset
 - Various scenarios

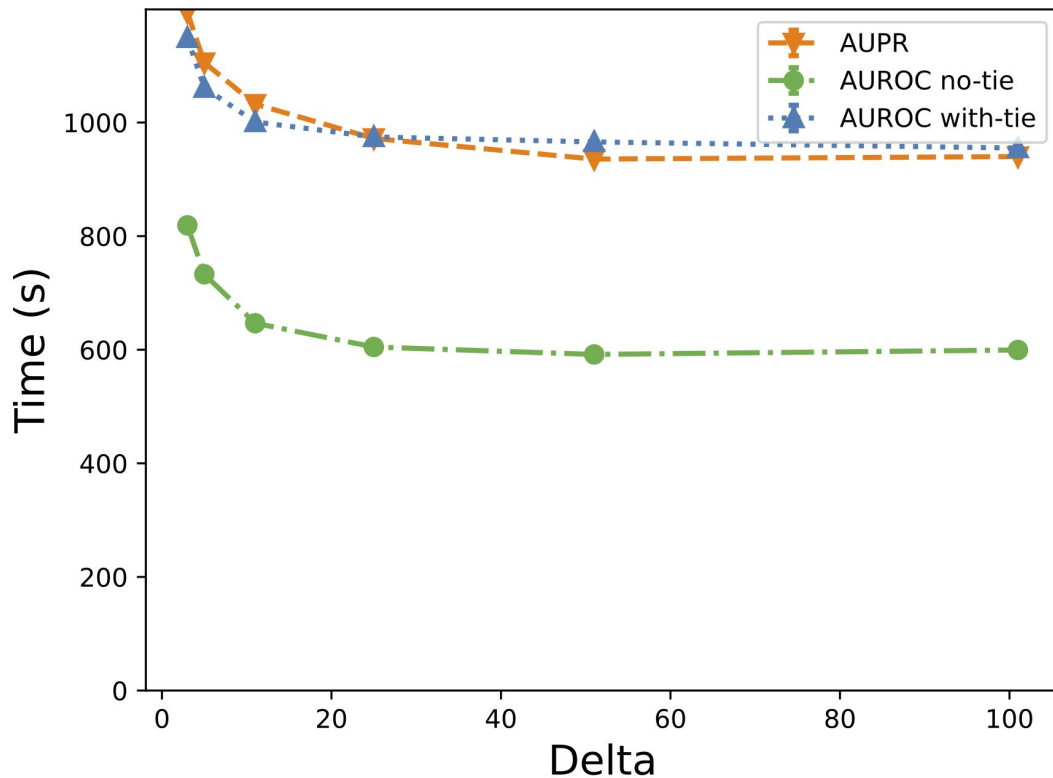
Results: Scalability to the Number of Samples



Results: Scalability to the Number of Parties



Results: Scalability to the Delta



Summary

- Not only the training and testing privately but also evaluation privately
- ppAURORA based on 3-party computation for AUC of ROC and PR curves
- Exact AUC result
- Linearly scalable to the number of samples and the parties
- Logarithmic decrease in the execution time parallel to the increase in delta

Thanks for listening!

Any Questions?

The icons in this presentation are from <https://www.flaticon.com/>

