Utility-Privacy Trade-off Curve

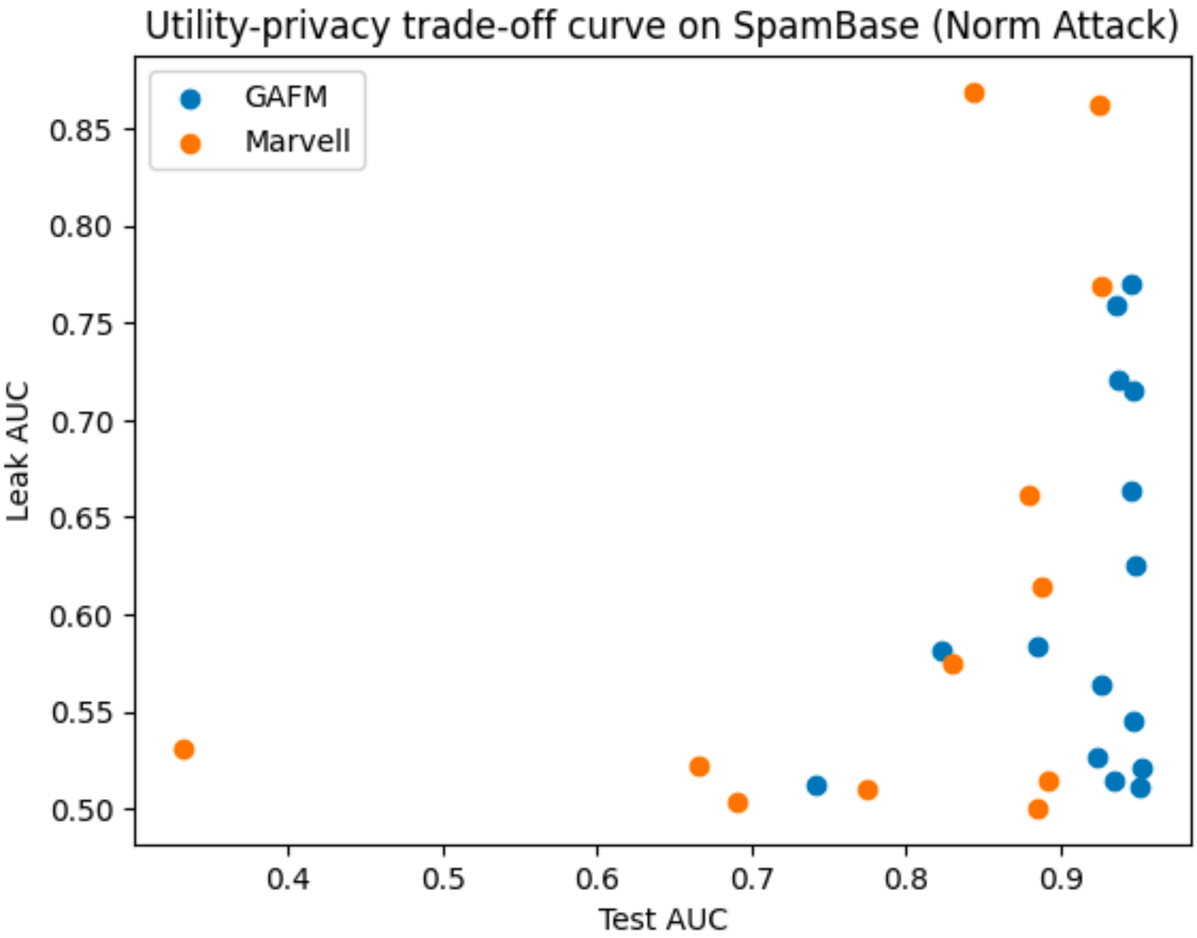
We take the Spambase dataset as an example to demonstrate the Utility-Privacy Trade-off Curve for Marvell and GAFM. The experimental settings for Marvell and GAFM are as follows:

- **Marvell**: According to the original Marvell paper, we adjust the range of parameter S to $S \in \{0.1, 0.25, 1, 4\}$, with each S repeated three times (seed = 0,1,2).
- **GAFM**: Similarly, we adjust the range of parameter Δ to $\Delta \in \{0.05, 0.1, 0.2, 0.3, 0.5\}$, with each Δ repeated three times. (The experimental results are directly from Appendix D.3 DISCUSSION ON Δ). (seed = 0,1,2).

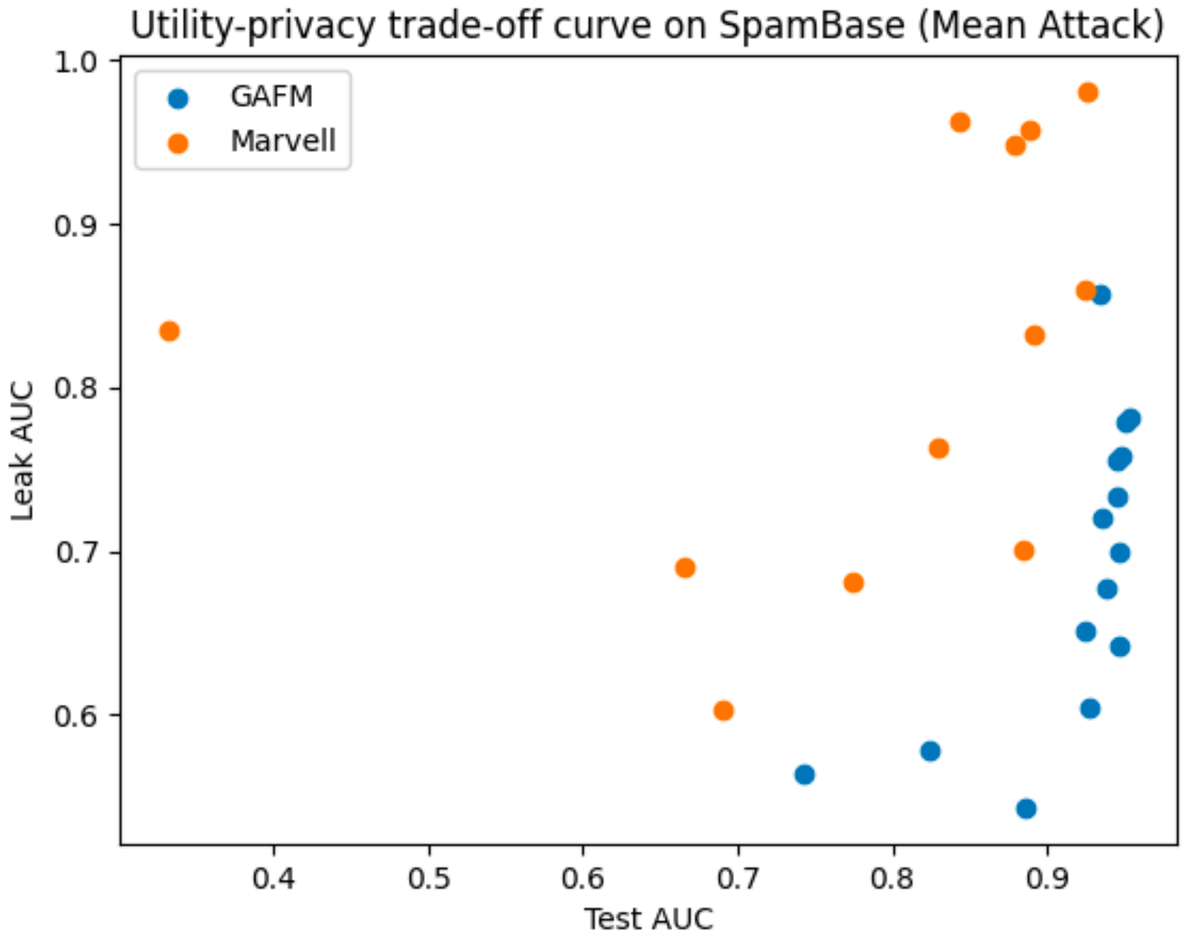
Plot the Test AUC-leak AUC curves for Marvell and GAFM under different attacks separately. We observe that, when facing three types of attacks, GAFM exhibits a better trade-off between utility and privacy compared to Marvell. Specifically, when the test AUC is close, GAFM has a lower leak AUC, or when the leak AUC is close, GAFM has a larger test AUC.

For Spambase data

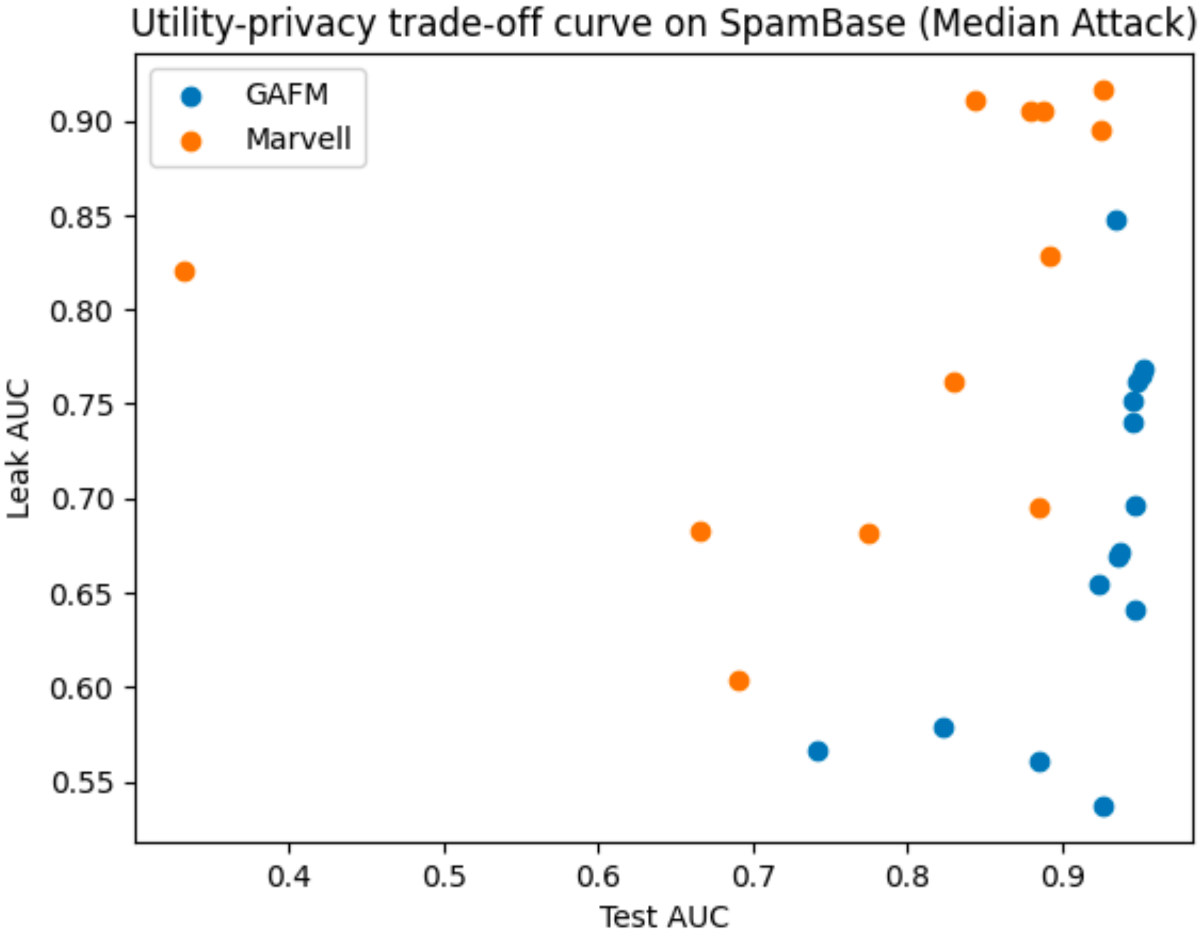
- **Norm Attack**



- **Mean Attack**

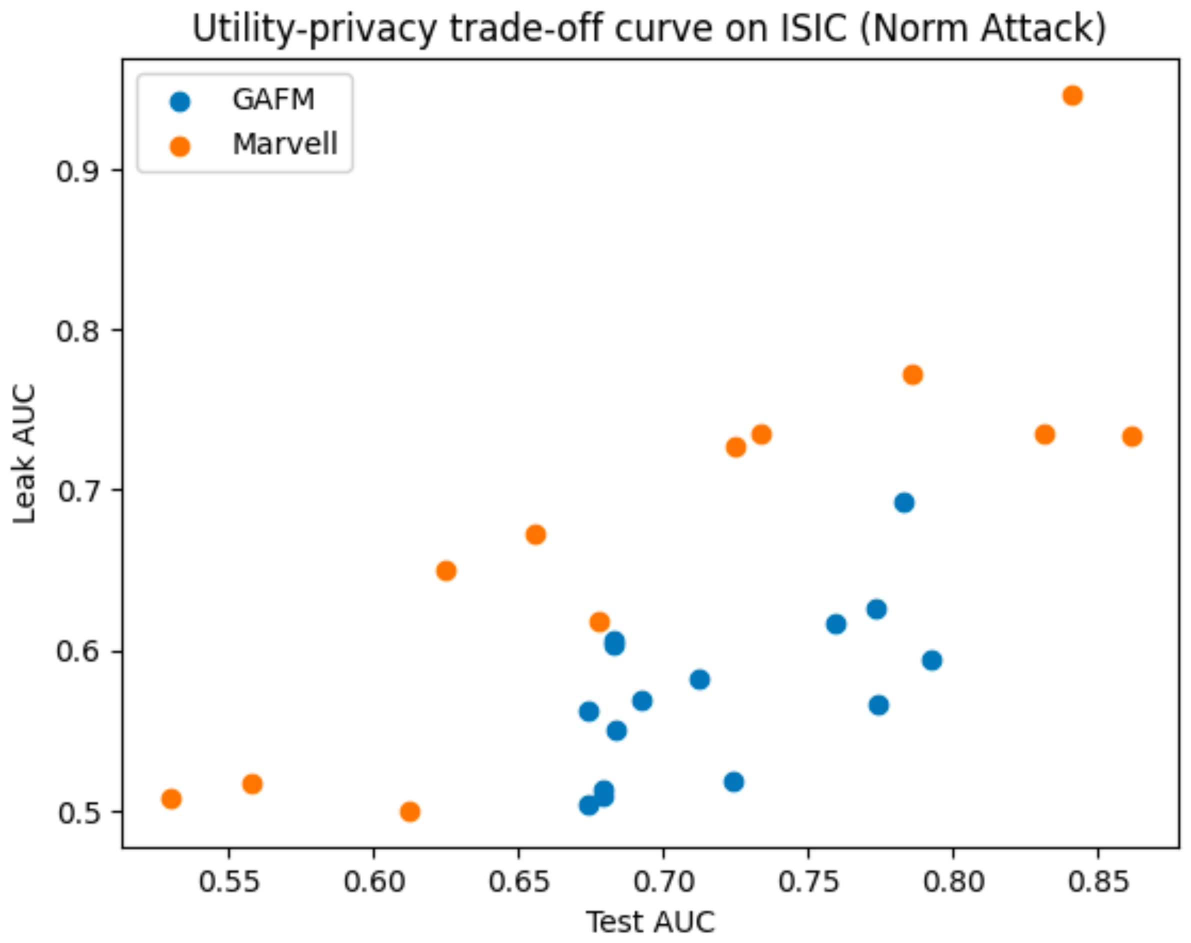


- **Median Attack**

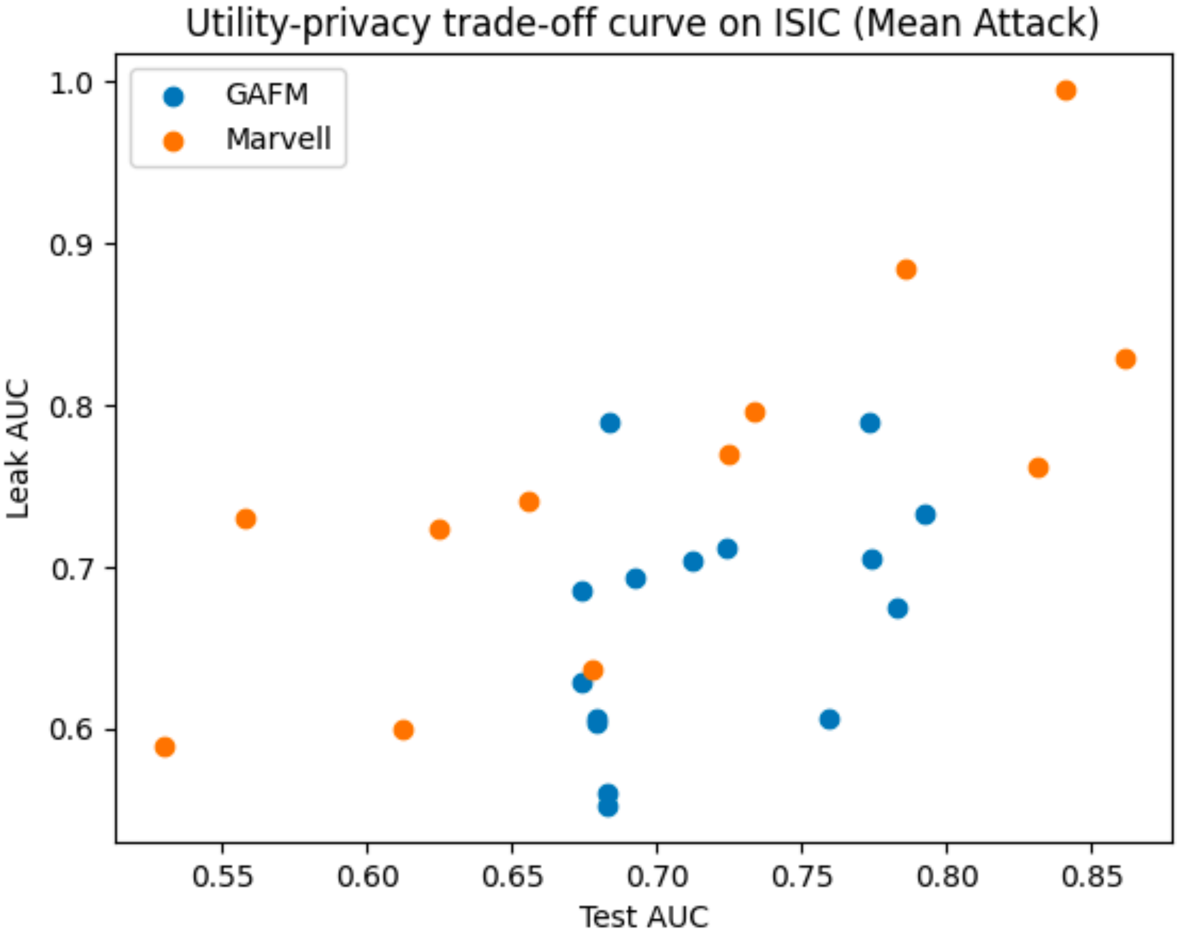


For ISIC data

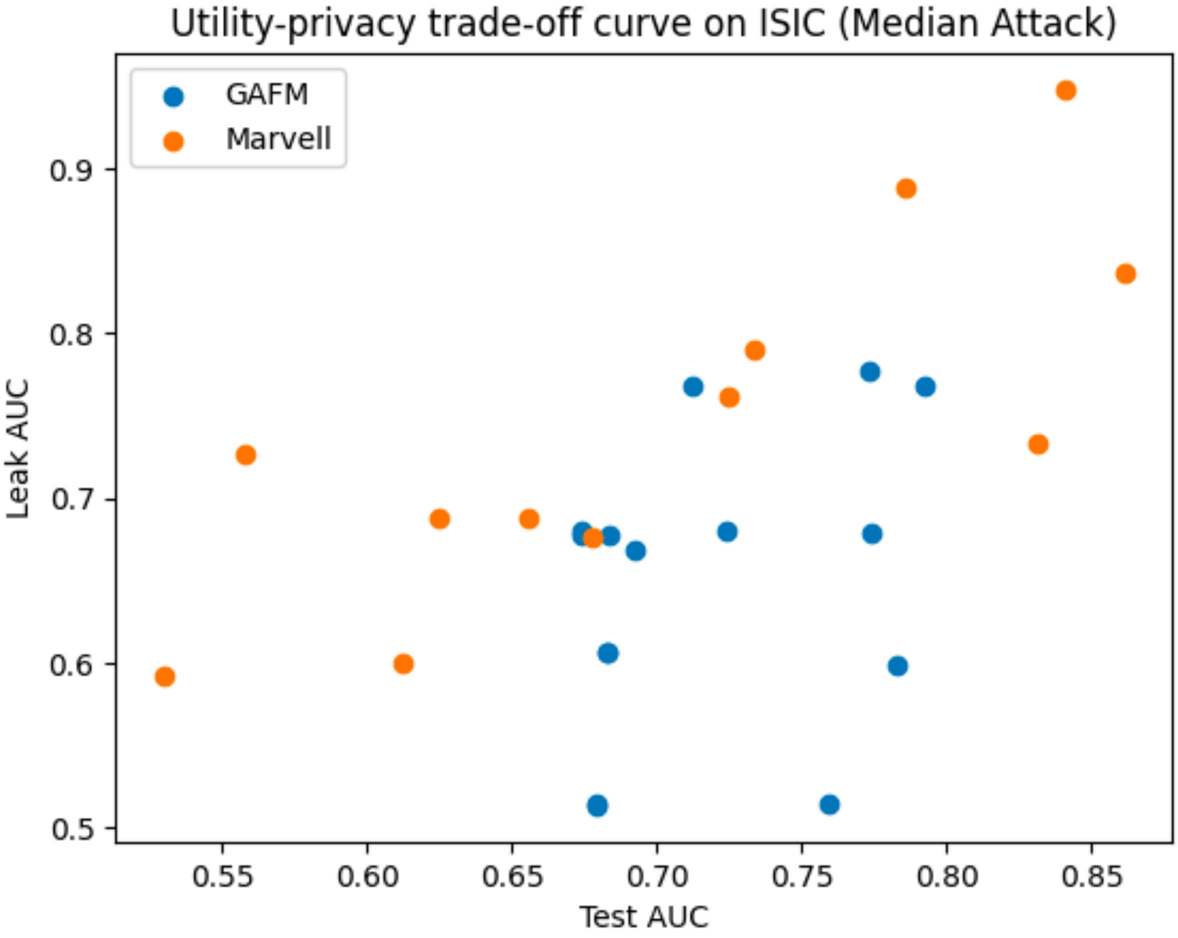
- **Norm Attack**


Utility-privacy trade-off curve on ISIC (Norm Attack)
● GAFM
● Marvell
0.9
0.8
0.7
0.6
0.5
Leak AUC
0.55
0.60
0.65
0.70
0.75
0.80
0.85
Test AUC

- **Mean Attack**



- **Median Attack**


Utility-privacy trade-off curve on ISIC (Median Attack)
● GAFM
● Marvell
Leak AUC
0.5
0.6
0.7
0.8
0.9
Test AUC
0.55
0.60
0.65
0.70
0.75
0.80
0.85