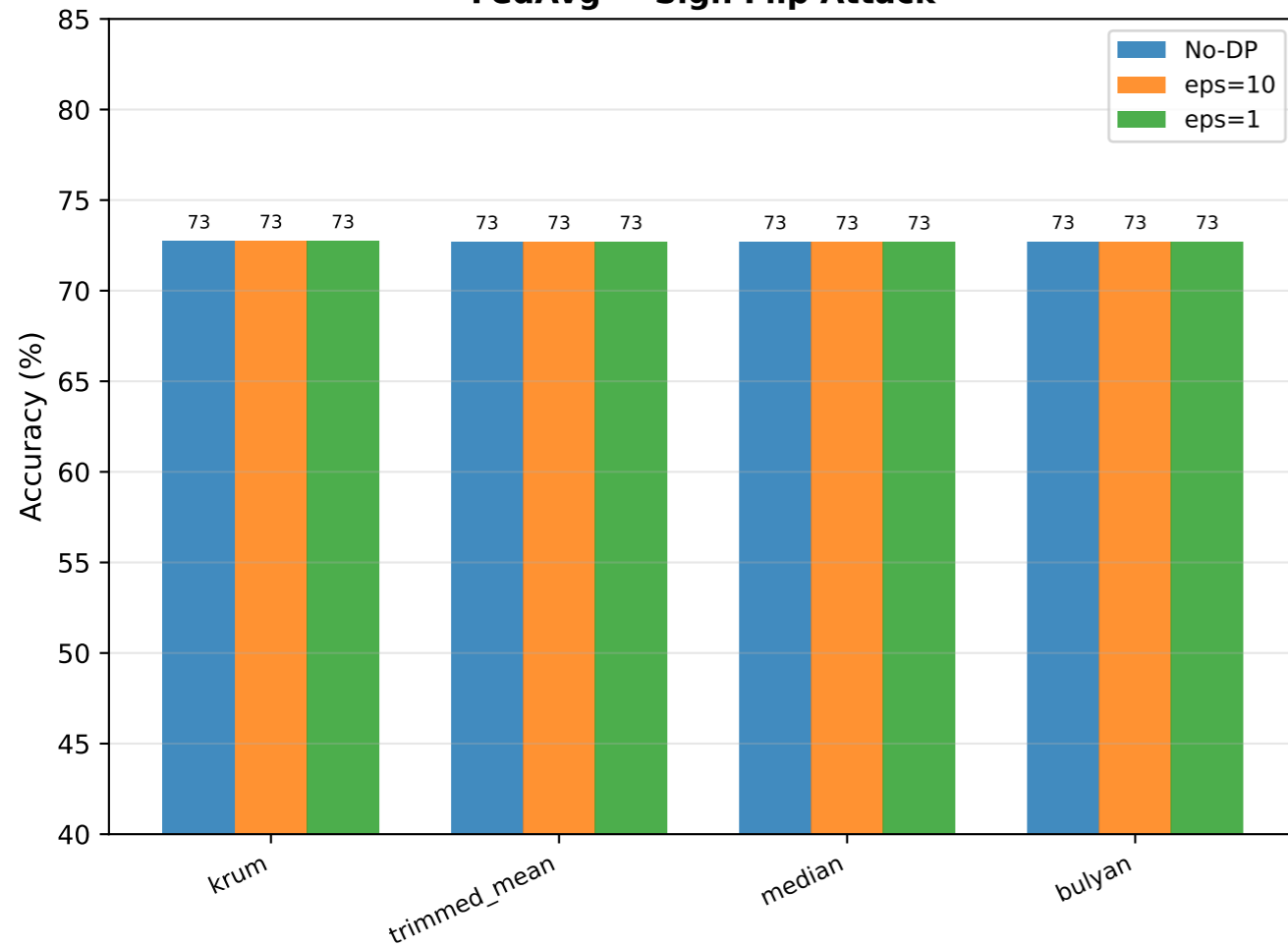


Byzantine Defense + DP Interaction (Cardiovascular)

Does DP noise help or hurt Byzantine robustness?

FedAvg — Sign Flip Attack



Ditto — Sign Flip Attack

