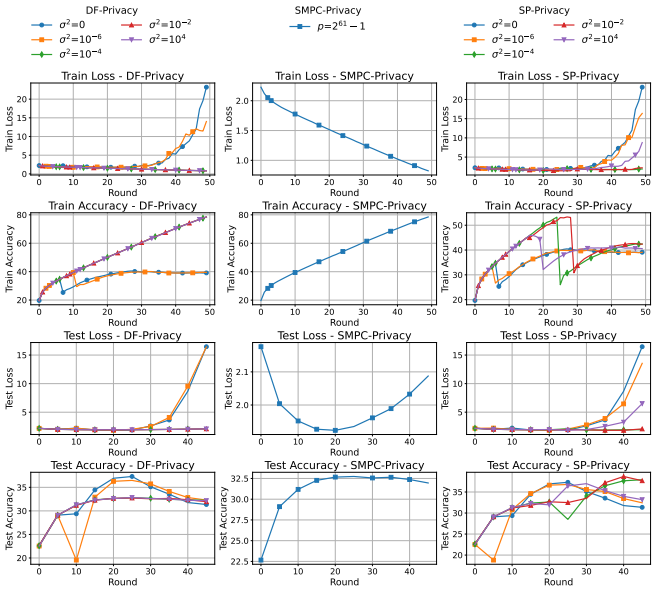
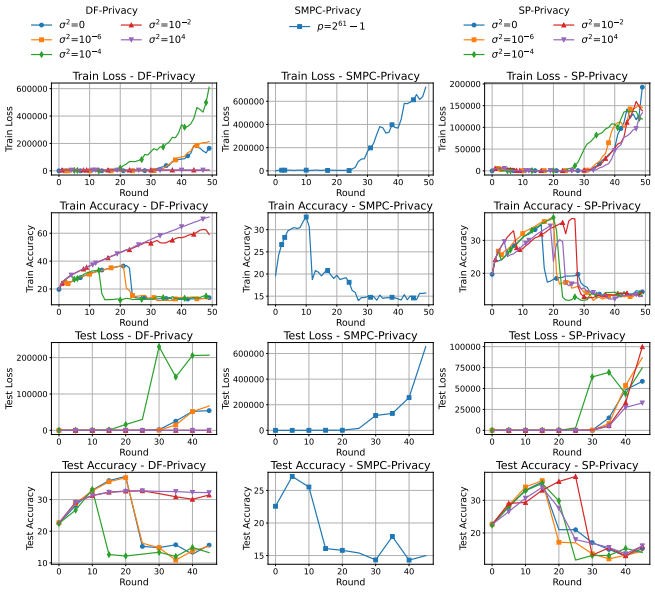
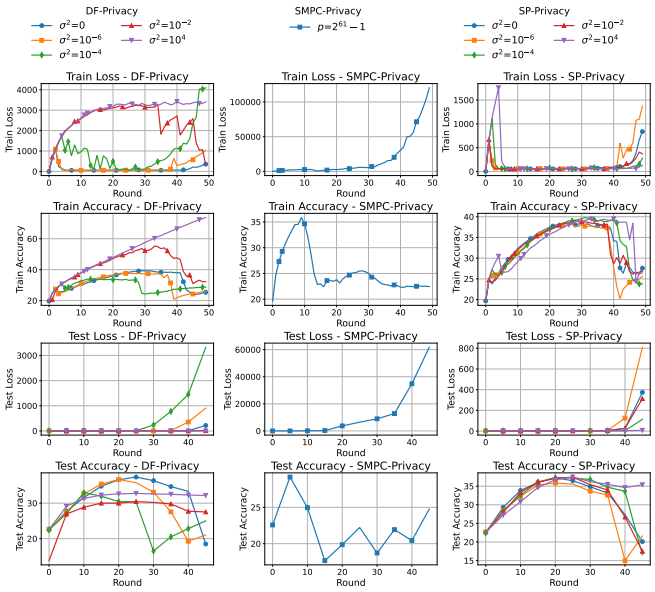
1 CIFAR-10



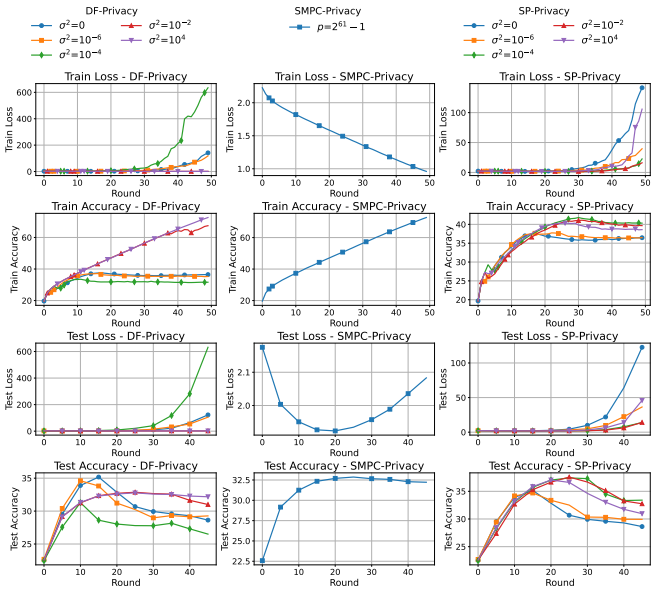
(a) No Attack



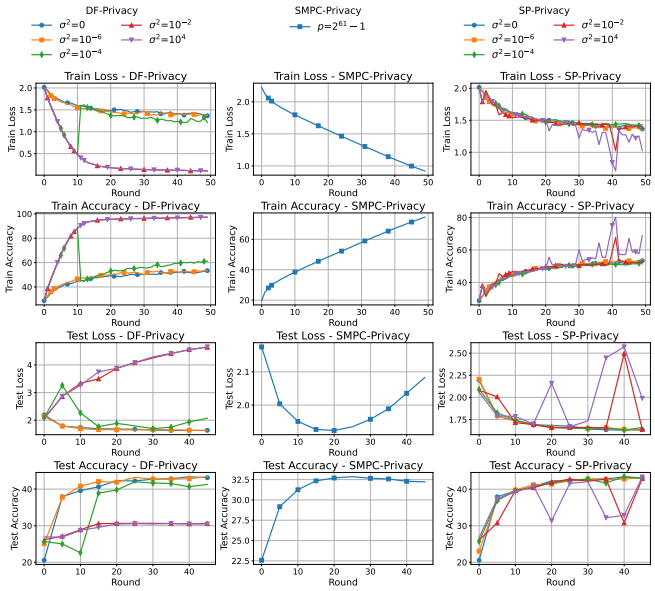
(b) Random Model Poisoning Attack



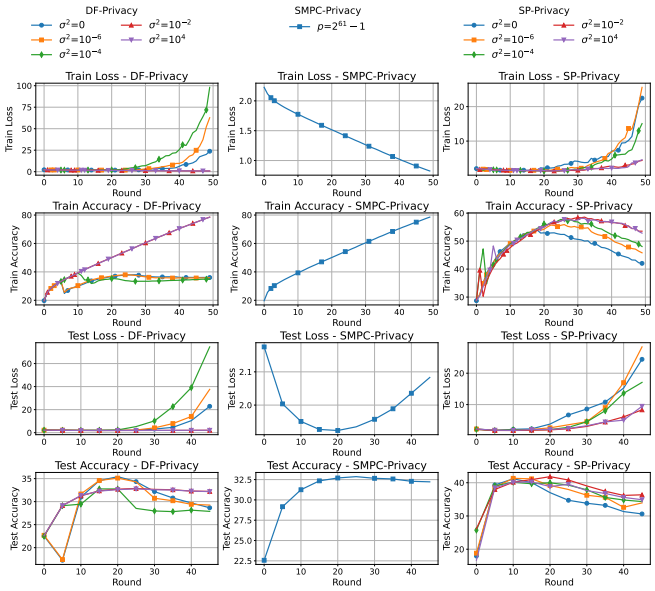
(c) Additive Gaussian Noise Attack



(d) ALIE Attack



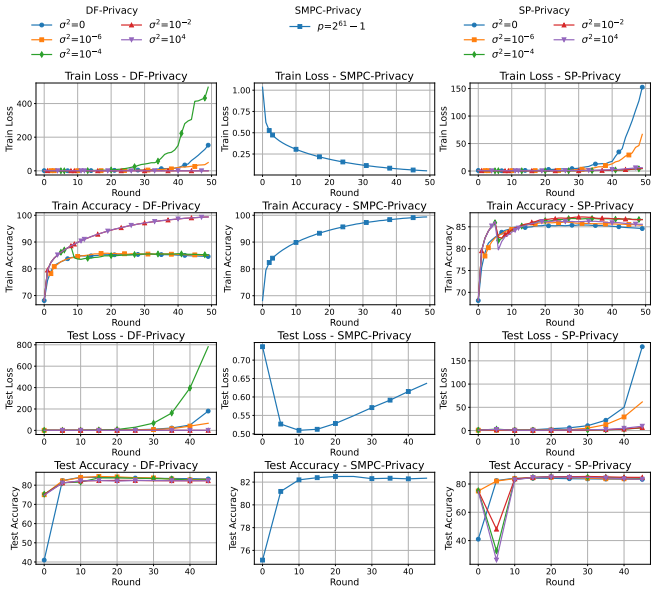
(e) Sign-Flipping Attack



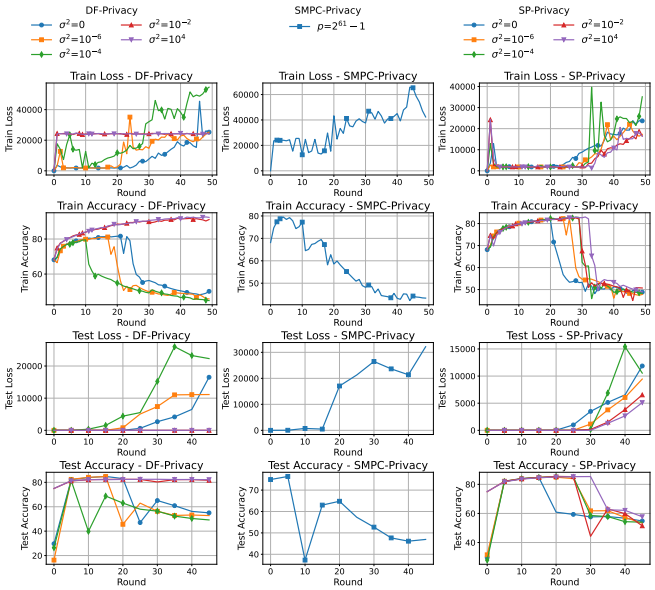
(f) Label-Flipping Attack

Figure 1: Testing and Training loss/accuracy for CIFAR-10 under different attacks.

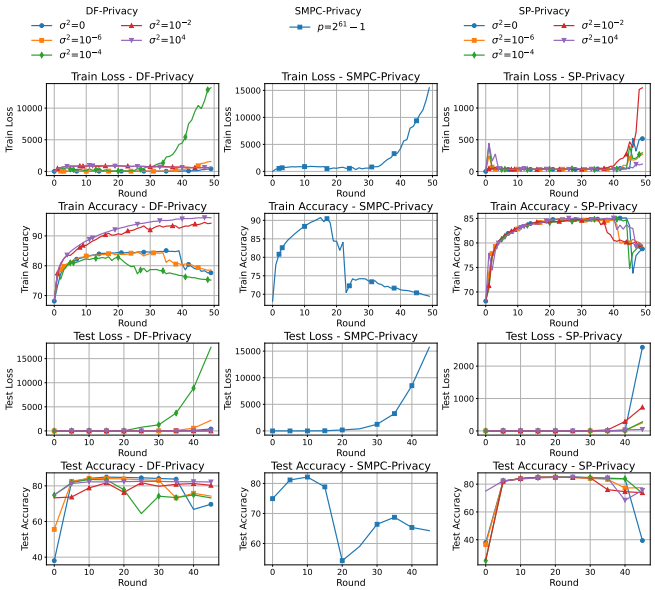
2 FashionMNIST



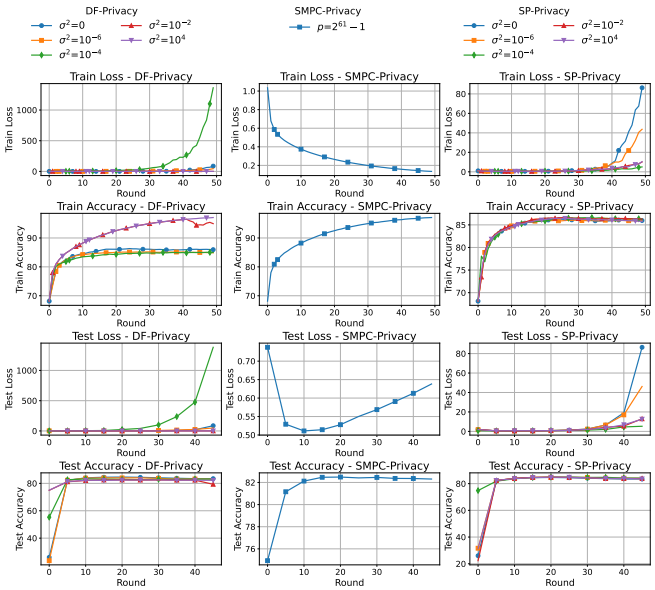
(a) No Attack



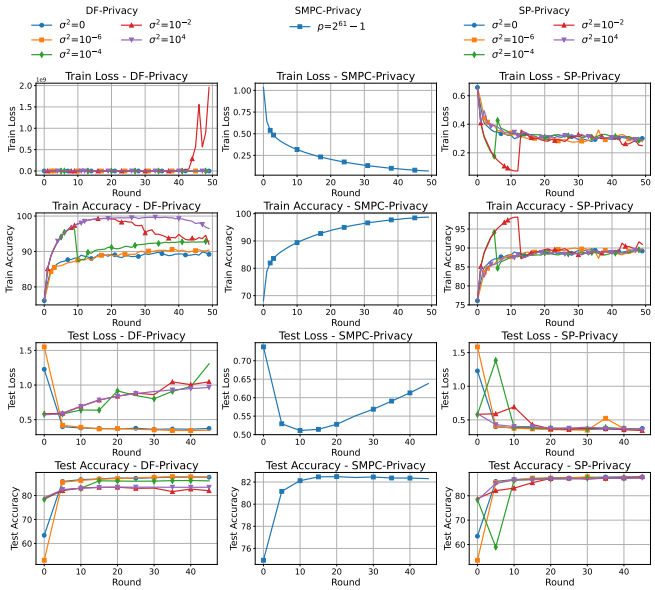
(b) Random Model Poisoning Attack



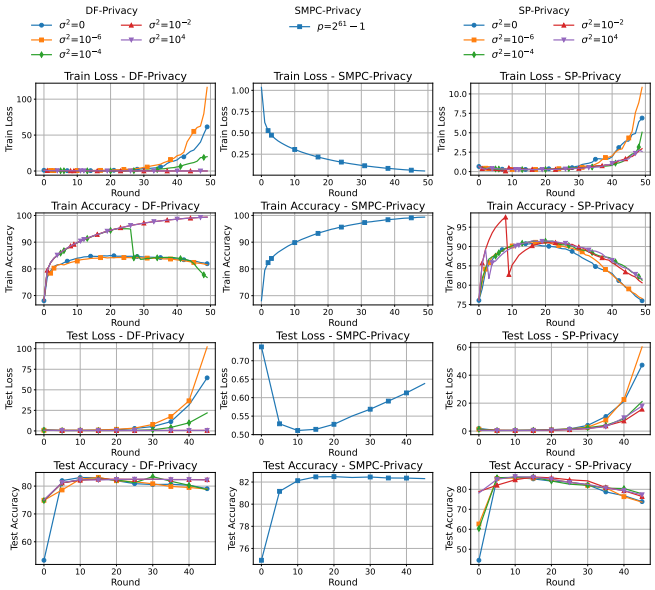
(c) Additive Gaussian Noise Attack



(d) ALIE Attack



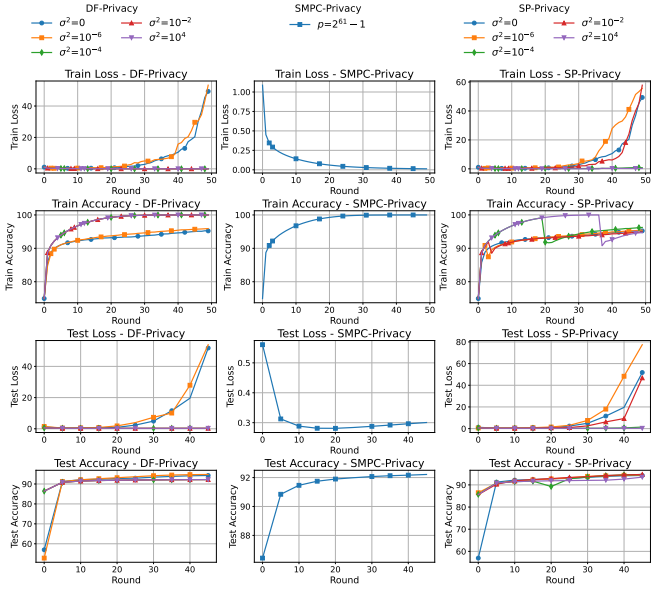
(e) Sign-Flipping Attack



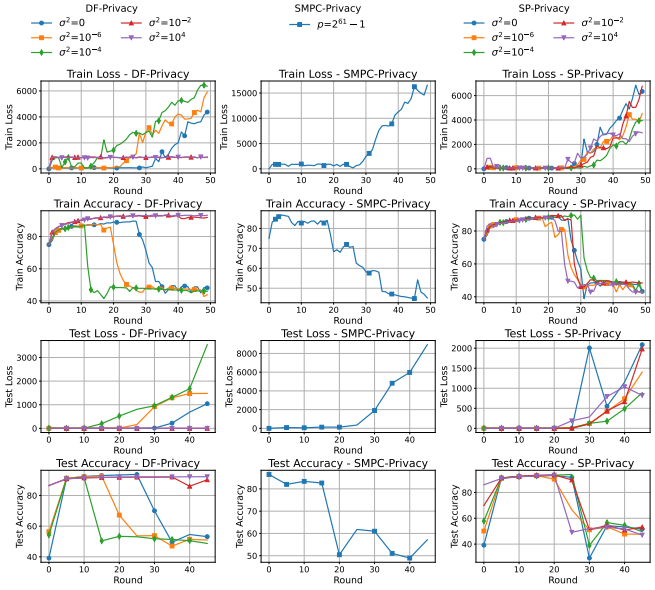
(f) Label-Flipping Attack

Figure 2: Testing and Training loss/accuracy for all privacy methods under different attacks with the FashionMNIST dataset.

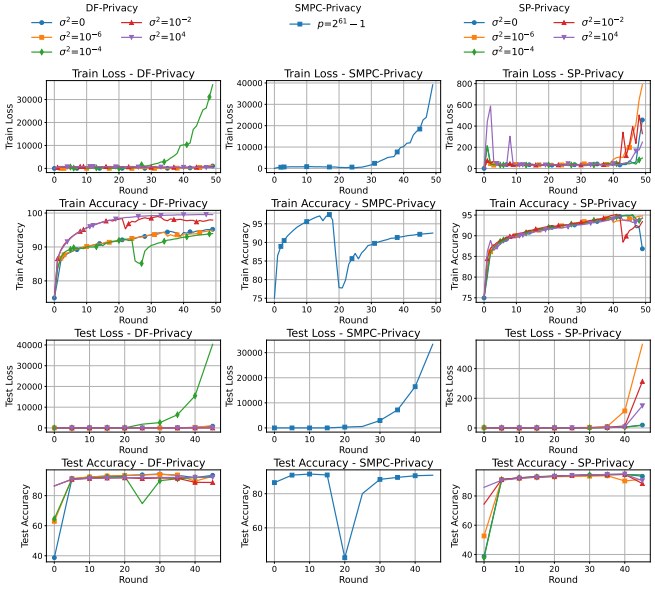
3 MINST



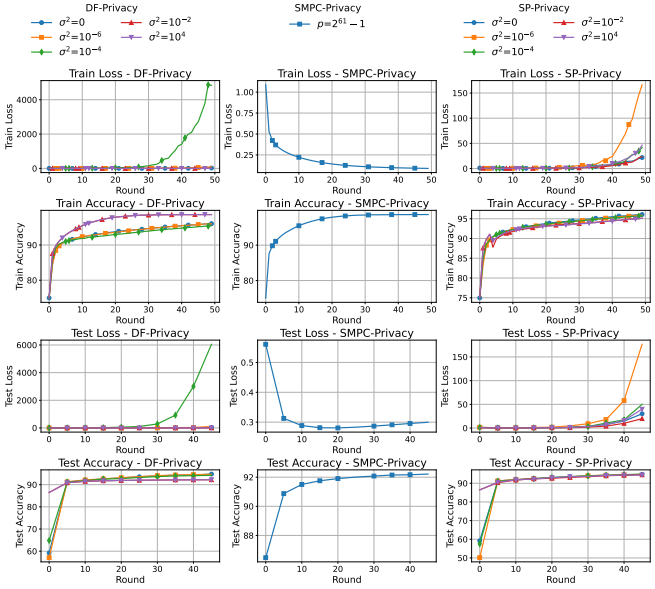
(a) No Attack



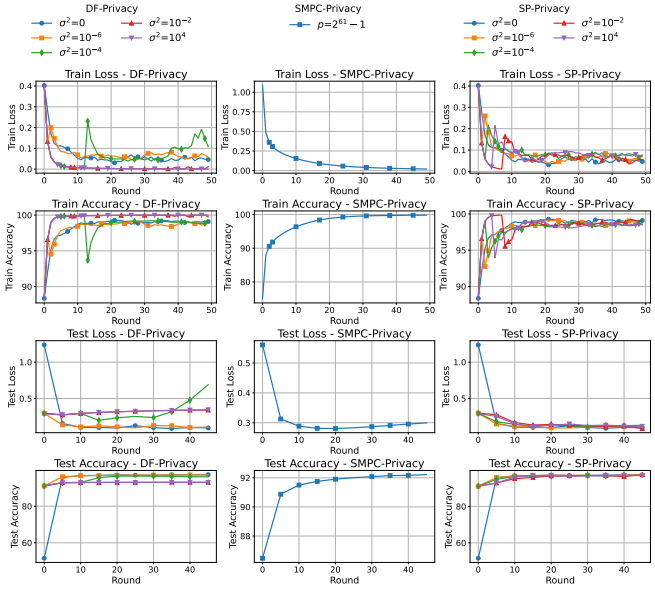
(b) Random Model Poisoning Attack



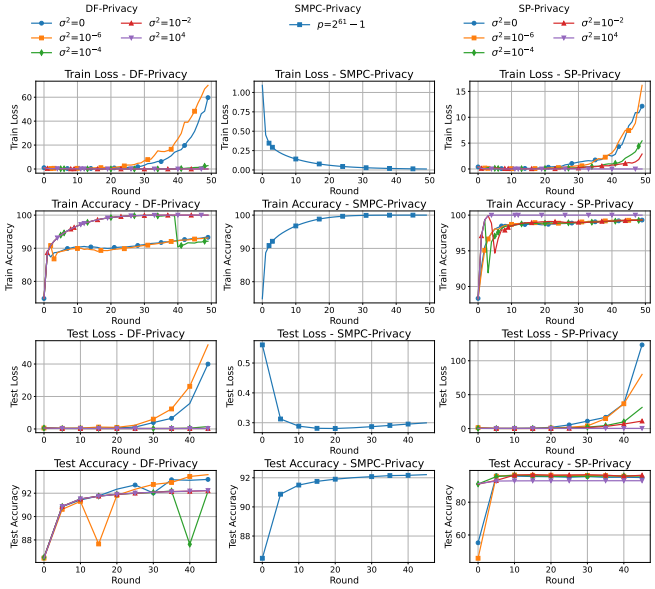
(c) Additive Gaussian Noise Attack



(d) ALIE Attack



(e) Sign-Flipping Attack



(f) Label-Flipping Attack

Figure 3: Testing and Training loss/accuracy for all privacy methods under different attacks with the MINST dataset.