

Data: MNIST  
Data: CIFAR100  
Data: CIFAR10  
Def: Gauss-out  
Def: Gauss-in  
Def: FSG  
Def: Controll  
Def: Controll  
Atk: Thresh  
Atk: Bix  
Atk: PGD  
Atk: HS  
Atk: FGM  
Atk: Deep

