Model	ResNet18	Pretrained on ImageNet
Optimizer	SGD	
Learning rate	0.001	
Batch size	32	

Method	Baseline			
Epochs	51			
Seed	**Benign**	**FGSM 8/255 black-box**	**AA Linf 4/255**	**Training time**
0	95.11	23.35	0	5239
1	95.13	22.18	0	5225
2	95.15	23.69	0	5308
3	95.1	22.46	0	5293
4	95.01	23.76	0	5282
Mean	**95.1**	**23.09**	**0**	**5269.4**
Std	0.05	0.72	0	35.71

Method	Isoreg		
Epochs	51		
Lambda	0.01		
Warm-up	1 epoch		
Epsilon	3.5		
Norm	Holder		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	21.14	20.68	25686
1	10.47	11.16	24871
2	12.33	10.58	24299
3	17.42	12.32	24679
4	69.43	33.15	25329
Mean	**26.16**	**17.58**	**24972.8**
Std	24.55	9.62	544.57

Method	Isoreg

Epochs	51
Lambda	0.001
Warm-up	1 epoch
Epsilon	3.5
Norm	Holder

Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	94.11	27.31	24709
1	94.27	25.95	24882
2	94.92	25.44	24318
3	94.51	25.5	24849
4	94.22	26.32	24716
Mean	**94.41**	**26.1**	**24694.8**
Std	0.32	0.76	224.42

Method	Isoreg
Epochs	51
Lambda	0.002
Warm-up	1 epoch
Epsilon	3.5
Norm	Holder

Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
5	93.09	28.27	25064
6	94.51	25.59	24493
7	93.68	27.78	23862
8	94.11	27.65	23188
9	93.4	29.38	22169
Mean	**93.76**	**27.73**	**23755.2**
Std	0.56	1.38	1129.87

Method	Temperature	*f_(x) = soft(alpha*s(x)) with alpha.detach()*
Epochs	51	
Warm-up	3 epoch	
Epsilon	1.74	

Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	92.62	24.16	24315
1	92.71	25.55	24113
2	92.77	25.47	22168
3	91.64	22.76	22573
4	92.38	26.37	23578
Mean	**92.42**	**24.86**	**23349.4**
Std	0.46	1.42	944.22

Method	Randbound		
Epochs	51		
Lambda	0.02		
Warm-up	1 epoch		
Epsilon	3.5		
Norm	Holder		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	80	20.72	9056
1	81.96	18.19	9087
2	81.84	19.86	8930
3	82.43	21.68	9046
4	80.05	19.03	9041
Mean	**81.26**	**19.9**	**9032**
Std	1.15	1.37	59.75

Method	Randbound		
Epochs	51		
Lambda	0.005		
Warm-up	1 epoch		
Epsilon	3.5		
Norm	Holder		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
5	91.94	23.33	9139
6	93.42	23.9	9425

7	93.38	23.84	9166
8	93.7	24.2	9252
9	93.22	22.33	9125
Mean	**93.13**	**23.52**	**9221.4**
Std	0.69	0.74	124.04

Method	Gnbound		
Epochs	51		
Lambda	0.005		
Warm-up	1 epoch		
Epsilon	3.5		
Std	16/255		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	93.61	27.57	9418
1	93.66	27.77	9637
2	93.16	29.36	9205
3	93.63	27.96	9231
4	93.37	28.98	9428
Mean	**93.49**	**28.33**	**9383.8**
Std	0.22	0.79	175.04

Method	Gn		
Epochs	51		
Warm-up	0 epoch		
Std	8/255		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	94.46	20.77	5414
1	94.47	21.13	5454
2	94.39	21.95	5427
3	94.7	21.65	5372
4	94.71	23.01	5254
Mean	**94.55**	**21.7**	**5384.2**
Std	0.15	0.86	78.57

Method	Gn		
Epochs	51		
Warm-up	0 epoch		
Std	16/255		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	93.05	30.46	5301
1	92.92	28.66	5325
2	92.98	29.92	5395
3	92.9	28.93	5510
4	93.18	29.85	5320
Mean	**93.01**	**29.56**	**5370.2**
Std	0.11	0.75	85.89

Method	FGSM		
Epochs	51		
Warm-up	0 epoch		
Std	8/255		
Seed	**Benign**	**FGSM 8/255 black-box**	**Training time**
0	61.79	61.62	8598
1	61.28	61.59	8624
2	61.8	62.95	8777
3	65.51	67.16	8592
4	64.99	64.74	8546
Mean	**63.07**	**63.61**	**8627.4**
Std	2.01	2.36	88.23

Method	Jacreg
Epochs	51
Lambda	1000
Warm-up	0 epoch
Norm	Holder

Seed	Benign	FGSM 8/255 black-box	Training time
0	95.11	23.35	24449
1	95.13	22.18	23756
2	95.15	23.69	24687
3	95.1	22.46	24887
4	95.01	23.76	24633
Mean	95.1	23.09	24482.4
Std	0.05	0.72	435.03

Method	Teacher
Epochs	51
Temp	20

Seed	Benign	FGSM 8/255 black-box	Training time
-5	94.52	23.28	5340
-4	94.02	28.07	5340
-3	94.21	25.89	5338
-2	94.04	27.01	5267
-1	94.03	27.78	5212
Mean	94.16	26.41	5299.4
Std	0.21	1.94	58.04

Method	Distillation
Epochs	51
Temp	20

Seed	Benign	FGSM 8/255 black-box	AA Linf 4/255	Training time
0	93.9	26.63	0	8110
1	94.13	27.39	0	8269
2	94.37	25.31	0	8261
3	93.89	26.65	0	8159
4	93.95	25.34	0	8124
Mean	94.05	26.26	0	8184.6
Std	0.2	0.91	0	75.59