Model LeNet *All attacks are black-box*
Optimizer SGD
Learning rate 0.001
Batch size 32

Method Baseline
Epochs 51

Seed	**Training time**	**Benign**	**PGD linf, 10, 0.01** 4/255	8/255	16/255	32/255
0	747	88.11	78.69	65.26	40.5	23.12
1	732	88.24	78.44	64.78	39.62	21.96
2	769	88.27	78.82	65.01	39.28	21.05
3	727	88.57	79.46	65.37	39.21	21.29
4	715	88.55	79.24	65.55	41	23.75
Mean	**738**	**88.35**	**78.93**	**65.19**	**39.92**	**22.23**
Std	20.78	0.2	0.41	0.3	0.79	1.17

Method Isoreg
Epochs 51
Lambda 0.1
Warm-up 1 epoch
Epsilon 3.5 *~16/255*
Norm Holder

Seed	**Training time**	**Benign**	**PGD linf, 10, 0.01** 4/255	8/255	16/255	32/255
0	3580	88.14	78.96	66.11	42.74	25.26
1	3650	88.12	78.22	65.07	40.88	24.08
2	3807	88.32	79.1	65.44	40.55	22.33
3	4029	88.6	79.47	66.07	41.14	22.95
4	3834	88.23	79.39	66.92	43.46	26.51
Mean	**3780**	**88.28**	**79.03**	**65.92**	**41.75**	**24.23**
Std	175.03	0.19	0.5	0.71	1.27	1.7

Method Isoreg

Epochs		51					
Lambda		3					
Warm-up	1 epoch						
Epsilon		3.5 *~16/255*					
Norm	Holder			**PGD linf, 10, 0.01**			
Seed	**Training time**	**Benign**		**4/255**	**8/255**	**16/255**	**32/255**
0	3981	71.24		63.59	53.85	38.97	29.44
1	4078	87.54		78.04	64.77	41.88	26.58
2	3828	86.49		78.3	67.1	47.3	30.97
3	3389	83.1		75.34	64.25	46.21	32.6
4	3304	82.87		74.65	64.53	47.88	34.55
Mean	**3716**	**82.25**		**73.98**	**62.9**	**44.45**	**30.83**
Std	350.17	6.49		6.03	5.18	3.86	3.04

Method	Isoreg						
Epochs		51					
Lambda		4					
Warm-up	1 epoch						
Epsilon		3.5 *~16/255*					
Norm	Holder			**PGD linf, 10, 0.01**			
Seed	**Training time**	**Benign**		**4/255**	**8/255**	**16/255**	**32/255**
5	3885	79.79		71.97	60.99	44.13	31.5
6	3479	81.49		72.19	61.51	43.85	30.99
7	3721	83.03		74.03	62.79	44.71	30.14
8	3919	69.68		62.03	52.54	37.73	28.51
9	3865	80.01		71.62	60.99	43.87	30.11
Mean	**3773.8**	**78.8**		**70.37**	**59.76**	**42.86**	**30.25**
Std	181.29	5.26		4.75	4.1	2.89	1.14

Method	Teacher						
Epochs		51					
Temp		20		**PGD linf, 10, 0.01**			
Seed	**Training time**	**Benign**		**4/255**	**8/255**	**16/255**	**32/255**

	-5	832	81.36	75.02	66.66	49.77	34.01
	-4	838	81.68	74.92	65.92	48.41	32.44
	-3	831	81.3	75.2	68	53.05	37.63
	-2	834	81.09	74.67	66.92	51.03	35.64
	-1	850	81.23	75.22	67.12	51.45	35.82
Mean		**837**	**81.33**	**75.01**	**66.92**	**50.74**	**35.11**
Std		7.75	0.22	0.23	0.75	1.75	1.97

Method	Distillation						
Epochs		51					
Temp		20		**PGD linf, 10, 0.01**			
Seed		**Training time**	**Benign**	**4/255**	**8/255**	**16/255**	**32/255**
	0	1385	79.07	74.1	68.37	56.36	43.22
	1	1391	79.69	74.22	67.63	53.91	39.31
	2	1394	78.97	74.74	69.71	59.59	47.77
	3	1385	78.98	74.02	68.27	56.21	42.46
	4	1380	79.29	74.34	68.16	56.13	42.61
Mean		**1387**	**79.2**	**74.28**	**68.43**	**56.44**	**43.07**
Std		5.52	0.3	0.28	0.77	2.03	3.03

Method	Gn						
Epochs		51					
Std	16/255			**PGD linf, 10, 0.01**			
Seed		**Training time**	**Benign**	**4/255**	**8/255**	**16/255**	**32/255**
	0	814	87.77	79.95	68.83	45.85	25.69
	1	837	87.68	80.17	68.5	44.65	24.67
	2	831	87.87	80.09	69.04	44.76	24.04
	3	833	88.12	80.55	69.77	45.54	24.13
	4	846	88.19	80.54	68.83	46.28	26.72
Mean		**832.2**	**87.93**	**80.26**	**68.99**	**45.42**	**25.05**
Std		11.69	0.22	0.27	0.47	0.7	1.14

Method	FGSM						
Epochs	51						
Budget	16/255		**PGD linf, 10, 0.01**				
Seed	**Training time**	**Benign**	**4/255**	**8/255**	**16/255**	**32/255**	
0	1410	83.95	82.64	81.26	77.84	70.94	
1	1425	84.11	82.92	81.6	77.89	70.16	
2	1433	84.05	82.66	81.17	77.72	69.93	
3	1410	84.23	83.1	81.68	78.28	70.6	
4	1403	84.33	83.04	81.56	78.54	72.33	
Mean	**1416.2**	**84.13**	**82.87**	**81.45**	**78.05**	**70.79**	
Std	12.36	0.15	0.21	0.22	0.34	0.94	