

Table 1

Dataset			OSSN	RKO	SVCM	BCOP
MNIST	Small	Clean	96.86 ± 0.13	97.28 ± 0.08	97.24 ± 0.09	97.54 ± 0.06
		Robust	42.95 ± 1.09	43.58 ± 0.44	28.94 ± 1.58	45.84 ± 0.90
	Large	Clean	98.31 ± 0.03	98.44 ± 0.05	97.93 ± 0.05	98.77 ± 0.05
		Robust	53.77 ± 1.02	55.18 ± 0.46	38.00 ± 1.82	56.66 ± 0.23
CIFAR10	Small	Clean	62.18 ± 0.66	61.77 ± 0.63	62.39 ± 0.46	64.53 ± 0.30
		Robust	48.03 ± 0.54	47.46 ± 0.53	47.59 ± 0.56	50.01 ± 0.21
	Large	Clean	67.51 ± 0.47	70.01 ± 0.26	69.65 ± 0.38	72.41 ± 0.22
		Robust	53.64 ± 0.49	55.76 ± 0.16	53.61 ± 0.51	58.72 ± 0.23

Table 2

Dataset		BCOP-Large	FC-3	KW-Large	KW-Resnet
MNIST	Clean	98.77 ± 0.05	98.71 ± 0.02	-	-
	Robust	56.66 ± 0.23	54.46 ± 0.30	-	-
CIFAR10	Clean	72.41 ± 0.22	62.60 ± 0.39	-	-
	Robust	58.72 ± 0.23	49.97 ± 0.35	-	-

Table 3

	KW	BCOP		KW	BCOP
Small			Small		
Clean	54.39	64.53 ± 0.30	Clean (*)	63.00	74.20 ± 2.23
PGD	49.94	51.26 ± 0.17	BA (*)	60.00	61.20 ± 2.99
FGSM	49.98	51.57 ± 0.18	PA (*)	63.00	74.00 ± 2.28
Large			Large		
Clean	60.14	72.41 ± 0.22	Clean (*)	68.00	77.60 ± 1.74
PGD	55.53	64.39 ± 0.26	BA (*)	64.00	71.20 ± 1.60
FGSM	55.55	64.53 ± 0.25	PA (*)	68.00	77.20 ± 1.60

Table 4-Maxmin-lr-0.0001

		OSSN	RKO	BCOP
Wasserstein Distance	MaxMin	7.39 ± 0.31	8.95 ± 0.12	9.91 ± 0.11

Table 4-ReLU-lr-0.001

		OSSN	RKO	BCOP
Wasserstein Distance	ReLU	7.06 ± 0.72	7.82 ± 0.21	8.28 ± 0.19

Table 7

Dataset			BCOP-Fixed	RK-L2NE	BCOP
MNIST	Small	Clean	93.57 ± 0.17	95.85 ± 0.12	97.54 ± 0.06
		Robust	7.51 ± 1.18	39.77 ± 0.73	45.84 ± 0.90
	Large	Clean	65.20 ± 3.94	96.76 ± 0.11	98.77 ± 0.05
		Robust	0.00 ± 0.00	37.79 ± 1.21	56.66 ± 0.23
CIFAR10	Small	Clean	50.61 ± 0.65	58.82 ± 0.67	64.53 ± 0.30
		Robust	36.44 ± 0.70	44.65 ± 0.61	50.01 ± 0.21
	Large	Clean	47.14 ± 0.38	56.75 ± 0.68	72.41 ± 0.22
		Robust	27.43 ± 1.26	43.40 ± 0.46	58.72 ± 0.23

Table 8

Dataset		BCOP-Large	FC-3	MMR-Universal
MNIST	Clean	98.77 ± 0.05	98.71 ± 0.02	-
	Robust	97.11 ± 0.07	97.06 ± 0.02	-
CIFAR10	Clean	72.41 ± 0.22	62.60 ± 0.39	-
	Robust	62.97 ± 0.30	53.67 ± 0.29	-

Table 9

Dataset		BCOP-Large	FC-3	QW-3	QW-4
MNIST	Clean	98.77 ± 0.05	98.71 ± 0.02	98.65	98.23
	Robust	56.66 ± 0.23	54.46 ± 0.30	42.13	27.59
	PGD	86.86 ± 0.25	81.96 ± 0.16	86.86	86.25
	FGSM	86.93 ± 0.20	83.64 ± 0.10	85.83	84.17
CIFAR10	Clean	72.41 ± 0.22	62.60 ± 0.39	79.15	77.15
	Robust	58.72 ± 0.23	49.97 ± 0.35	44.46	31.41
	PGD	64.39 ± 0.26	50.05 ± 0.36	72.07	71.89
	FGSM	64.53 ± 0.25	50.21 ± 0.34	72.11	71.92