

Classification error (%) on the first 1000 test samples						
model	original images	mnist		original images	fashion_mnist	
		adversarial images attack	gray-box		adversarial images attack	gray-box
UNENCRYPTED	A	CW l_2	100.00	8.30	CW l_2	100.00
		CW l_0	100.00		CW l_0	100.00
		CW l_∞	100.00		CW l_∞	100.00
	B	FGSM	39.50	9.50	FGSM	77.20
PERMUTATED	A	CW l_2	4.50	12.30	CW l_2	12.70
		CW l_0	7.30		CW l_0	12.50
		CW l_∞	5.40		CW l_∞	12.90
	B	FGSM	8.60	12.00	FGSM	29.80
AES · ECB	A	CW l_2	irrelevant	54.60	CW l_2	irrelevant
	B	FGSM		55.30	FGSM	
AES · CBC	A	CW l_2	irrelevant	71.50	CW l_2	irrelevant
	B	FGSM		90.30	FGSM	
AES · CTR	A	CW l_2	4.20	17.40	CW l_2	17.20
	B	FGSM	4.90	16.70	FGSM	26.50