

Classification error (%) on the first 1000 test samples							
model		original images	mnist		original images	fashion_mnist	
			adversarial attack	images gray-box		adversarial attack	images gray-box
UNENCRYPTED	A	1.49	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	2.10	FGSM	39.50	9.50	FGSM	77.20
PERMUTATED	A	3.70	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	4.20	FGSM	8.60	12.00	FGSM	29.80
AES · ECB	A	18.40	CW l_2		54.60	CW l_2	
	B	19.30	FGSM		55.30	FGSM	
AES · CBC	A	67.60	CW l_2	irrelevant	71.50	CW l_2	irrelevant
	B	87.40	FGSM		90.30	FGSM	
AES · CTR	A	3.70	CW l_2	4.20	17.40	CW l_2	17.20
	B	2.70	FGSM	4.90	16.70	FGSM	26.50