

| | | | mnist | | fashion_mnist | |
|-------------|-----------------|------------|----------|-----------------|---------------|-----------------|
| | | | original | attacked | original | attacked |
| UNENCRYPTED | CW I_2 | | | 100 | | 100 |
| | CW I_0 | | 0.97 | 100 | 8.66 | 100 |
| | CW I_∞ | | | 100 | | 100 |
| | FGSM | | 1.5 | | 10.62 | |
| PERMUTATED | CW I_2 | | | | | |
| | CW I_0 | | 3.63 | | 12.4 | |
| | CW I_∞ | | | | | |
| | FGSM | | 3.02 | | 12.04 | |
| ECB | CW ₁ | encrypt v1 | 16.58 | | 55.66 | not interesting |
| | | encrypt v2 | 18.11 | | 41.97 | |
| | CW ₂ | encrypt v1 | 16.71 | | 55.35 | |
| | | encrypt v2 | 17.81 | | 41.47 | |
| | FGSM | encrypt v1 | 20.88 | | 59.23 | |
| | | encrypt v2 | 19.95 | | 46.25 | |
| CBC | CW ₁ | encrypt v1 | 64.07 | not interesting | 72.12 | not interesting |
| | | encrypt v2 | 69.12 | | 64.47 | |
| | CW ₂ | encrypt v1 | 63.76 | | 90 | |
| | | encrypt v2 | 88.65 | | 90 | |
| | FGSM | encrypt v1 | 88.65 | | 90 | |
| | | encrypt v2 | 88.65 | | 90 | |
| CTR | CW ₁ | encrypt v1 | 88.65 | not interesting | 90 | not interesting |
| | | encrypt v2 | 88.65 | | 90 | |
| | CW ₂ | encrypt v1 | 88.65 | | 90 | |
| | | encrypt v2 | 88.65 | | 90 | |
| | FGSM | encrypt v1 | 88.65 | | 90 | |
| | | encrypt v2 | 88.65 | | 90 | |

Permutated accuracies on different image sizes (used padding with 0's to increase size)

| | image size | error rate | min/epoch |
|---------------|------------|------------|-----------|
| mnist | 28x28 | 3.63 | 4 |
| | 40x40 | 2.65 | 5 |
| | 60x60 | 2.69 | 12 |
| | 100x100 | 2.3 | 14 |
| fashion_mnist | 28x28 | 12.4 | |
| | 40x40 | 12.07 | 13 |
| | 60x60 | | |
| | 100x100 | | |