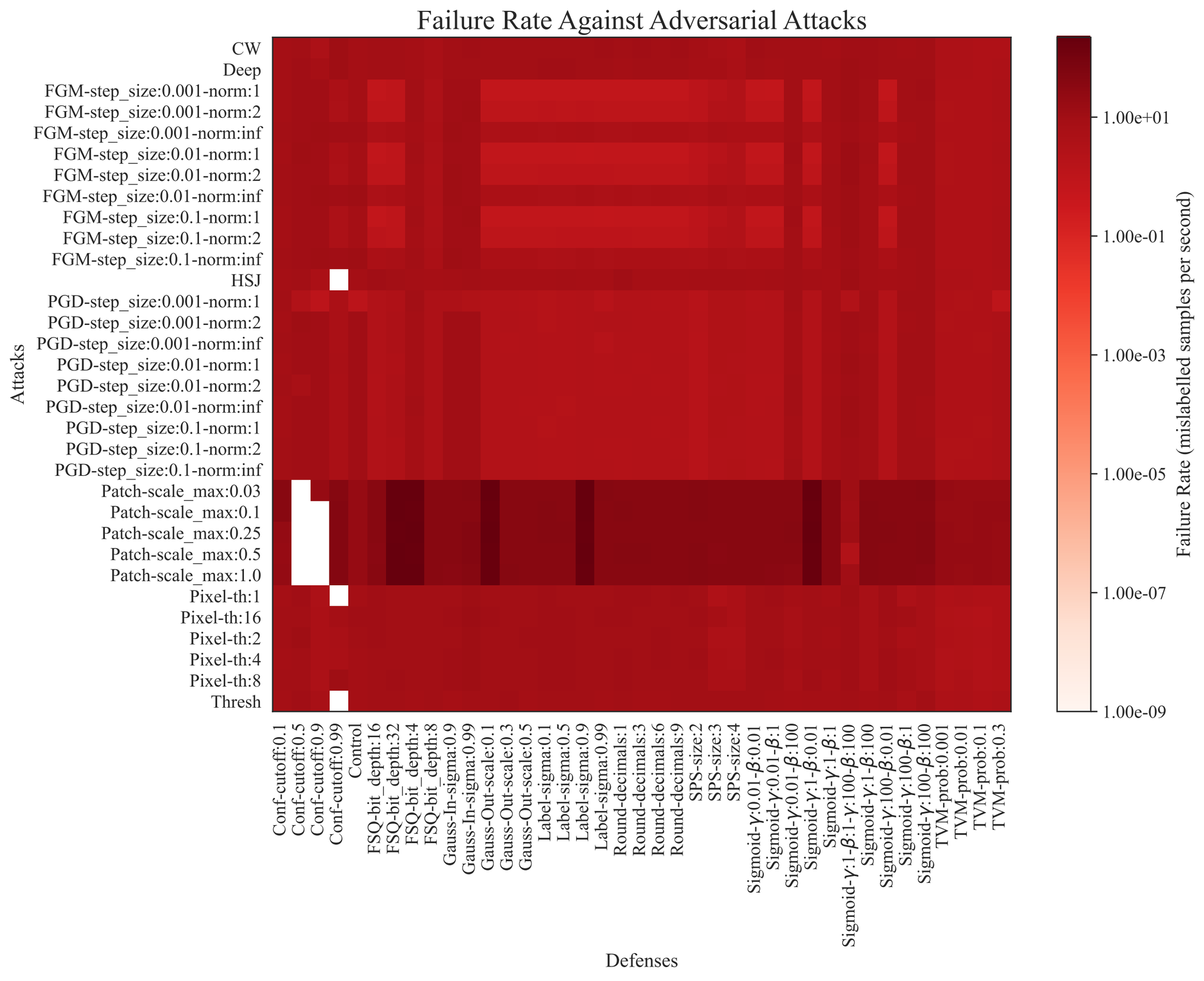
Failure Rate Against Adversarial Attacks
Attacks
CW
Deep
FGM-step_size:0.001-norm:1
FGM-step_size:0.001-norm:2
FGM-step_size:0.001-norm:inf
FGM-step_size:0.01-norm:1
FGM-step_size:0.01-norm:2
FGM-step_size:0.01-norm:inf
FGM-step_size:0.1-norm:1
FGM-step_size:0.1-norm:2
FGM-step_size:0.1-norm:inf
HSJ
PGD-step_size:0.001-norm:1
PGD-step_size:0.001-norm:2
PGD-step_size:0.001-norm:inf
PGD-step_size:0.01-norm:1
PGD-step_size:0.01-norm:2
PGD-step_size:0.01-norm:inf
PGD-step_size:0.1-norm:1
PGD-step_size:0.1-norm:2
PGD-step_size:0.1-norm:inf
Patch-scale_max:0.03
Patch-scale_max:0.1
Patch-scale_max:0.25
Patch-scale_max:0.5
Patch-scale_max:1.0
Pixel-th:1
Pixel-th:16
Pixel-th:2
Pixel-th:4
Pixel-th:8
Thresh
Conf-cutoff:0.1
Conf-cutoff:0.5
Conf-cutoff:0.9
Conf-cutoff:0.99
Control
FSQ-bit_depth:16
FSQ-bit_depth:32
FSQ-bit_depth:4
FSQ-bit_depth:8
Gauss-In-sigma:0.9
Gauss-In-sigma:0.99
Gauss-Out-scale:0.1
Gauss-Out-scale:0.3
Gauss-Out-scale:0.5
Label-sigma:0.1
Label-sigma:0.5
Label-sigma:0.9
Label-sigma:0.99
Round-decimals:1
Round-decimals:3
Round-decimals:6
Round-decimals:9
SPS-size:2
SPS-size:3
SPS-size:4
Sigmoid-γ:0.01-β:0.01
Sigmoid-γ:0.01-β:1
Sigmoid-γ:0.01-β:100
Sigmoid-γ:1-β:0.01
Sigmoid-γ:1-β:1
Sigmoid-γ:1-β:1-γ:100-β:100
Sigmoid-γ:1-β:100
Sigmoid-γ:100-β:0.01
Sigmoid-γ:100-β:1
Sigmoid-γ:100-β:100
TVM-prob:0.001
TVM-prob:0.01
TVM-prob:0.1
TVM-prob:0.3
Defenses
Failure Rate (mislabelled samples per second)
1.00e+01
1.00e-01
1.00e-03
1.00e-05
1.00e-07
1.00e-09