Understanding the Cause of Adversarial Vulnerability

- imperfect risk
- concentration
- uncertain inputs

$1 - \text{Risk}$

with $\mathcal{F}_{\alpha}$

with $\mathcal{F}_{\alpha,\gamma}$

RobustBench models
[Croce+, 2021]

Adversarial Robustness (y-axis)

Risk (x-axis)