

Preventing distillation-based attacks on Neural Network IP

Grailoo, Mahdiah; Abideen, Zain Ul; Leier, Mairo; Pagliarini, Samuel Nascimento arXiv.org 2022 / 7 p. : ill

<https://doi.org/10.48550/arXiv.2204.00292>