

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>

A tutorial on design obfuscation : from transistors to systems

Pagliarini, Samuel Nascimento 2021 IEEE 22nd Latin American Test Symposium (LATS), Punta del Este, Uruguay, 27-29 October

2021 2021 / 3 p. : ill <https://doi.org/10.1109/LATS53581.2021.9651741>