

### **Hardware Trojans for confidence reduction and misclassifications on neural networks**

Grailoo, Mahdiah; **Leier, Mairo; Pagliarini, Samuel Nascimento** Proceedings Of The Twenty Third International Symposium On Quality Electronic Design (ISQED 2022) 2022 / art. 180541, p. 230-235 <https://doi.org/10.1109/ISQED54688.2022.9806246>

### **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>