24th Australian Institute of Physics Congress

Contribution ID: **204**

Type: **Talk (preferred)**

Quantum Enhanced Robustness in Adversarial Machine Learning

Tuesday 13 December 2022 14:30 (15 minutes)

Machine learning models are susceptible to *adversarial examples* - inputs to the model which have been manipulated in order to confuse it. We study the vulnerability and resiliency of quantum classifiers to such inputs.

Author: Mr WEST, Maxwell (The University of Melbourne)

Co-authors: Mr TSANG, Shu Lok (The University of Melbourne); Mr LOW, Jia Shun (The University of Melbourne); Dr HILL, Charles (The University of Melbourne); Prof. SEVIOR, Martin (The University of Melbourne); Prof. LECKIE, Christopher (The University of Melbourne); Prof. HOLLENBERG, Lloyd (The University of Melbourne); Dr ERFANI, Sarah (The University of Melbourne); Dr USMAN, Muhammad (The University of Melbourne)

Presenter: Mr WEST, Maxwell (The University of Melbourne)

Session Classification: AIP: Quantum Science and Technology

Track Classification: AIP Congress: AIP: Quantum Science and Technology