香港浸會大學 HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE 計算機科學系

35 YEARS OF EXCELLENCE

DEPARTMENT OF COMPUTER SCIENCE

SEMINAR

2023 SERIES

Adversarially Robust Deep Neural Networks

DATE & TIME

29 SEP 2023 (FRI) 11:30 AM – 12:30 PM

VENUE

WLB 210, The Wing Lung Bank Building for Business Studies,
Shaw Campus

PROF. CHANG XU

Senior Lecturer
School of Computer Science
University of Sydney

ABSTRACT

New deep learning techniques keep improving accuracy on many benchmark tasks. However, deep neural networks' weaknesses have been criticized for a while. As we chase higher accuracy, we must also think about balancing accuracy and robustness. In this talk, I'll present our recent work on making neural networks more resistant to attacks. We're asking: if we have a well-trained accurate neural network, how can we make it tougher against attacks without spending too much? Specifically, for the latest vision transformer neural networks, how can we regain the balance between accuracy and toughness? We'll go back to the start of network training and suggest a novel random approach. This method naturally makes the network more resistant to attacks.

SPEAKER'S BIOGRAPHY

REGISTER NOW

Enquiries: 3411-2385 **Email:** comp@comp.hkbu.edu.hk **Website:** https://bit.ly/bucs-events