香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

**TMLR Young Scientist SEMINAR**

**2023 SERIES**

**Trustworthy Machine Learning and Reasoning Group**


## Dr. Junyuan Hong

Postdoctoral Fellow,
VITA Group,
IFML & WNCG at UT Austin.


**Date: 09 Sept 2023 (Saturday)**

**Time: 09:00 – 10:40 (HKT)**

**Meeting: https://hkbu.zoom.us/j/6603117755**

---

# Backdoor Meets Data-Free Learning

## ABSTRACT


Data-free learning emerges as an effective method when sensitive training data cannot be shared together with trained models for downstream tasks. Meanwhile, backdoor injection is a rising concern when data are not well curated and prone to be poisoned. In this talk, we will discuss the positive and negative consequences when backdoor meets data-free learning. (1) For the negative side, we show that backdoor can transfer from a teacher model to a student model by data-free distillation, which implies new risks in distillation from large pre-trained models. (2) For the positive side, we show that backdoors can be injected into models without access to training data, which enables post-hoc IP protection by watermarking without maintaining sensitive training data.


## BIOGRAPHY

Junyuan Hong is a postdoctoral fellow hosted by Dr. Zhangyang Wang in the VITA group, Institute for Foundations of Machine Learning (IFML) and Wireless Networking and Communications Group (WNCG) at UT Austin. Junyuan obtained his Ph.D. degree from Computer Science and Engineering at ILLIDAN Lab@Michigan State University (MSU), advised by Dr. Jiayu Zhou. Previously, he earned his B.S. in Physics and M.S. in Computer Science at University of Science and Technology of China (USTC).

## ENQUIRY


Email: bhanml@comp.hkbu.edu.hk