

# YIREN (AARON) ZHAO

yaz21@cam.ac.uk

UK Contact: (0044) 07547842218

## EDUCATION

---

<b>University of Cambridge, Cambridge, UK</b> <i>PhD in Computer Science</i>	<i>Grad. 2022</i>
<b>University of Cambridge, Cambridge, UK</b> <i>Master of Philosophy in Advanced Computer Science, Award of Distinction</i>	<i>Grad. 2017</i>
<b>Imperial College London, London, UK</b> <i>Bachelor of Engineering in Electrical &amp; Electronic Engineering, First Class Honors</i>	<i>Grad. 2016</i>

## SELECTED AWARDS AND HONORS

---

<b>Research Fellowship at St John's College, University of Cambridge</b> This prestigious Fellowship (up to four years) offers an opportunity to carry out independent research with financial support from the College.	<i>2021</i>
<b>Apple Scholar in AI and ML</b> A global program created to recognize the contributions of emerging leaders in computer science and engineering at the graduate level. Received a fellowship award of around 120,000 USD from Apple Inc..	<i>2020</i>
<b>EPSRC International Doctoral Studentship joint University of Cambridge Computer Laboratory Qualcomm Premium Scholarship</b> Fully funded PhD scholarship for 3.5 years.	<i>2017</i>
<b>Willis Jackson Medal and Prize</b> For excellence in academic performance, one award per academic year.	<i>2016</i>

## EXPERIENCE

---

<b>Department of Electrical and Electronic Engineering and Imperial X, Imperial College London, Assistant Professor</b> <ul style="list-style-type: none"><li>Lead a team looking at problems at the intersections between ML, hardware and security.</li><li>Supervise Undergraduate, Master and PhD students.</li></ul>	<i>2022 - Now</i>
<b>Department of Computer Science, University of Cambridge, Visiting Researcher</b> <ul style="list-style-type: none"><li>A visiting researcher in both the Computer Architecture and ML group.</li><li>Supervise Undergraduate, Master and PhD students.</li></ul>	<i>2022 - Now</i>
<b>Department of Computer Science, University of Cambridge, Research Fellow</b> <ul style="list-style-type: none"><li>Research on how Machine Learning on unstructured, complex data types, and the potential implications to hardware systems.</li><li>Plan and write research grant applications. Supervise Master and PhD students.</li></ul>	<i>2021 - 2022</i>
<b>Apple AI and ML, Part-time Contractor</b> Manager: Xin Wang and Francesco Rossi <ul style="list-style-type: none"><li>Direct report to Apple ML compiler (middleware) team lead.</li><li>Investigate research-orientaged projects.</li></ul>	<i>Dec 2021 - June 2022</i>
<b>Microsoft Research New England, Part-time Contractor</b> Manager: Dr. Nicolo Fusi <ul style="list-style-type: none"><li>Working on Project AutoML</li><li>Design novel hardware-aware AutoML methods</li></ul>	<i>June 2019-Feb 2020</i>

Microsoft Research New England, Research Intern

June 2019-Oct 2020

Supervisor: Dr. Nicolo Fusi

- Working on Project AutoML

Microsoft Research Redmond, Research Intern

June 2018-Oct 2018

Supervisor: Dr. Daniel Lo and Dr. Eric Chung

- Working on Project Catapult and Project Brainwave. Design and implement novel compression techniques for neural network training
- Filed several US patents for the proposed novel DNN compression techniques

Microsoft Research Cambridge, Research Intern

June 2017-Oct 2017

Supervisor: Dr. Hitesh Ballani

- Working on Project Sirius. Design and research on new routing methods between racks in a datacenter

## PAPERS & THESIS

---

### **DAdaQuant: Doubly-adaptive quantization for communication-efficient Federated Learning**

R Honig, Y Zhao and R Mullins

International Conference on Machine Learning 2022 (ICML 2022)

### **Rapid Model Architecture Adaption for Meta-Learning**

Y Zhao, X Gao, I Shumailov, N Fusi and R Mullins

in submission, 2021

### **Markpainting: Adversarial Machine Learning meets Inpainting**

D Khachaturov, I Shumailov, Y Zhao, D Bates, N Papernot, R Mullins and R Anderson

International Conference on Machine Learning 2021 (ICML 2021)

### **Manipulating SGD with Data Ordering Attacks**

I Shumailov, Z Shumaylov, D Kazhdan, Y Zhao, N Papernot, M A Erdogdu, R Anderson

Thirty-fifth Conference on Neural Information Processing Systems (NeurIPS 2021)

### **Learned Low Precision Graph Neural Networks**

Y Zhao\*, D Wang\*, D Bates, R Mullins, P Lio and M Jamnik

The 1st Workshop on Machine Learning and Systems (EuroMLSys 2021)

### **Sponge Examples: Energy-Latency Attacks on Neural Networks**

I Shumailov\*, Y Zhao\*, D Bates, N Papernot, R Mullins and R Anderson

6th IEEE European Symposium on Security and Privacy (EuroS&P 2021)

### **Probabilistic Dual Network Architecture Search on Graphs**

Y Zhao\*, D Wang\*, X Gao, R Mullins, P Lio and M Jamnik

Deep Learning on Graphs: Methods and Applications (*Best student paper award*, DLG-AAAI'21)

### **Towards Certifiable Adversarial Sample Detection**

I Shumailov\*, Y Zhao\*, R Mullins and R Anderson

13th ACM Workshop on Artificial Intelligence and Security 2020 (AISEC 2020)

### **Pay Attention to Features, Transfer Learn Faster CNNs**

K Wang\*, X Gao\*, Y Zhao, X Li, D Dou, X Gao, and C Xu

International Conference on Learning Representations 2020 (ICLR 2020)

### **Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information**

Y Zhao\*, I Shumailov\*, C Han, X Gao, R Mullins and R Anderson

IEEE International Conference on Dependable Systems and Networks Workshops (DSN-W 2020)

### **Focused Quantization for Sparse DNNs**

Y Zhao\*, X Gao, R Mullins and C Xu

Thirty-third Conference on Neural Information Processing Systems (NeurIPS 2019)

### **Sitatapatra: Blocking the Transfer of Adversarial Samples**

I Shumailov\*, X Gao\*, Y Zhao\*, R Mullins, R Anderson and C Xu

in submission

### **Automatic Generation of Multi-precision Multi-arithmetic CNN Accelerators for FPGAs**

Y Zhao\*, X Gao\*, X Guo\*, J Liu, E Wang, R Mullins, P Cheung, G Constantinides and C Xu

International Conference on Field Programmable Technology (ICFPT 2019)

### **The Taboo Trap: Behavioural Detection of Adversarial Samples**

I Shumailov\*, Y Zhao\*, R Mullins and R Anderson  
in submission

**Characterizing Sources of Ineffectual Computations in Deep Learning Networks**

M Nikolic, M Mahmoud, Y Zhao, R Mullins and A Moshovos  
International Symposium on Performance Analysis of Systems and Software 2019 (ISPASS 2019)

**Dynamic Channel Pruning: Feature Boosting and Suppression**

X Gao\*, Y Zhao\*, R Mullins and C Xu  
International Conference on Learning Representations 2019 (ICLR 2019)

**To compress or not to compress: Understanding the Interactions between Adversarial Attacks and Neural Network Compression**

Y Zhao\*, I Shumailov\*, R Mullins and R Anderson  
The Conference on Systems and Machine Learning 2019 (SysML 2019)

**Mayo: A Framework for Auto-generating Hardware Friendly Deep Neural Networks**

Y Zhao\*, X Gao\*, R Mullins and C Xu  
2nd International Workshop on Embedded and Mobile Deep Learning (Workshop of Mobisys) (EMDL 2018)

**Redundancy-Reduced MobileNet Acceleration on Reconfigurable Logic For ImageNet Classification**

J Su, J Faraone, J Liu, Y Zhao, D Thomas, P Leong and P Cheung  
14th International Symposium on Applied Reconfigurable Computing (ARC 2018)

**An Efficient Implementation of Online Arithmetic**

Y Zhao, J Wickerson and G Constantinides  
2016 International Conference on Field-Programmable Technology (ICFPT 2016)

**Improving Compression Pipelines For Convolutional Neural Networks**

Master thesis

\* indicates equal contribution

PATENTS

---

**Neural Network Activation Compression with Narrow Block Floating-point**

D Lo, A Phanishayee, E S Chung, Y Zhao and R Zhao  
US patent, US20200210838, 2020

**Neural Network Activation Compression with Non-uniform Mantissas**

D Lo, A Phanishayee, E S Chung, Y Zhao  
US patent, US20200242474, 2020

**Neural network Activation Compression with Outlier Block Floating-point**

D Lo, A Phanishayee, E S Chung, Y Zhao and R Zhao  
US patent, US20200210839, 2020

**Adjusting Activation Compression for Neural Network Training**

D Lo, B D Rouhani, E S Chung, Y Zhao, A Phanishayee and R Zhao  
US patent, US20200264876, 2020

TEACHING AND SUPERVISIONS

---

**Efficient Adversarial Training (Final year project)**

Maximilian Kaufmann, jointly supervised with Ilia Shumailov

*2021-2022*

**Backdoors in Neural Networks (Final year project)**

Mikel Bober, jointly supervised with Ilia Shumailov

*2021-2022*

**Reducing communication costs in Federated Learning (Final year project)**

Robert Honig, jointly supervised with Prof. R Mullins

*2020-2021*

**Hardware-informed differentiable neural architecture search (Master project)**

Karl Otness, jointly supervised with Prof. R Mullins

*2019-2020*

**Replay Attacks on Reinforcement Learning (Final year project)**

Timothy Lazarus, jointly supervised with Prof. R Mullins and Ilia Shumailov

*2019-2020*