

Hassan Dbouk

✉ hdbouk2@illinois.edu | 📞 +1(415)980-9969 | 🌐 <https://hassandbouk.web.illinois.edu>

EDUCATION

University of Illinois at Urbana-Champaign
Ph.D. in Electrical and Computer
Engineering

2017 - present | Urbana, IL

expected graduation: December 2022

GPA : 3.97/4

Thesis: Robust and Efficient Deep
Learning: Algorithms, Architectures, and
Circuits

American University of Beirut

B.E. in Computer and Communications
Engineering

2013 - 2017 | Beirut, Lebanon

Minor in Mathematics

High Distinction and a 4.0 GPA

SKILLS

Python • PyTorch • C/C++ • Matlab •
Verilog • Cadence Tools

SELECTED PUBLICATIONS¹

• H. Dbouk, et. al, "Adversarial Vulnerability of Randomized Ensembles" **ICML**, 2022.

• H. Dbouk, et. al, "Generalized Depthwise-Separable Convolutions for Adversarially Robust and Efficient Neural Networks" **NeurIPS**, 2021.

• H. Dbouk, et. al, "DBQ: A Differentiable Branch Quantizer for Lightweight Deep Neural Networks" **ECCV**, 2020.

• H. Dbouk, et. al, "A 0.44-uJ/dec, 39.9-us/dec, Recurrent Attention In-Memory Processor for Keyword Spotting", **JSSC**, 2020

• H. Dbouk, et. al, "0.34 uJ/decision 18 k decisions/s Recurrent Attention In-memory Processor for Keyword Spotting", **CICC**, 2020

• H. Dbouk, et. al, "Low-complexity Fixed-point Convolutional Neural Networks for Automatic Target Recognition", **ICASSP**, 2020

KEY COURSES

Random Processes • Statistical Learning Theory • Computational Inference & Learning • Advanced DSP • Integer Programming • Coding Theory • Information Theory • Intro to Optimization • Vector Space Signal Processing • ML in Silicon • Analog IC Design • Digital IC Design • Computer Organization

¹ Full list of publications at my Google Scholar page

RESEARCH EXPERIENCE

University of Illinois at Urbana-Champaign (UIUC)

Research Assistant | 2017 – present

Supervised by Professor Naresh Shanbhag

Research Interests: machine learning, adversarial robustness, signal processing, efficient inference, hardware acceleration.

◊ **Adversarial Robustness of Randomized Ensembles (ICML'22)**

- Established fundamental bounds on the adversarial robustness of randomized ensembles. (*work under review*)
- Showed that existing adaptive attacks provide a *false* sense of robustness and proposed a provably-consistent and efficient adversarial attack algorithm capable of compromising randomized ensembles.
- Broke the state-of-the-art defense (BAT) using our adaptive attack.
- Comprehensive experiments on CIFAR-10/100, SVHN, and ImageNet datasets were conducted to verify our claims.

◊ **Accelerating Robust CNNs on Edge GPUs (NeurIPS'21 - Spotlight)**

- Proposed Generalized Depthwise-Separable (GDWS) convolutions for post-training acceleration of robust deep networks.
- Developed theoretically optimal and efficient approximation algorithms for constructing GDWS convolutions under complexity and error constraints.
- Demonstrated *massive* (2 – 3×) improvements in frames-per-second via extensive experiments on CIFAR-10, SVHN, and ImageNet datasets using an NVIDIA Jetson Xavier.

◊ **Keyword Spotting Acceleration (CICC'20 & JSSC'20)**

- Designed and taped-out an IC to implement our *recurrent attention*-based algorithm for key-word spotting (KWS). The IC integrates both compute in-memory (IMC) and digital processing for optimal resource allocation.
- Demonstrated the lowest reported *measured* decision latency of 40μs KWS using the Google Speech dataset while achieving <0.5μJ per decision.

Texas Instruments - Kilby labs

Research Intern | Summers 2019 & 2020 | Dallas, TX

Supervised by Dr. Mahesh Mehendale

◊ **Ternary Network Quantization (ECCV'20)** Proposed a differentiable branch quantization algorithm for training accurate and compressed deep networks that are optimized for ternary-based arithmetic Edge devices.

◊ **Hardware-aware Network Training** Modeled and integrated various circuit accurate noise models into PyTorch for enabling the deployment of accurate and compressed deep nets onto error-prone mixed-signal hardware platforms.

Carnegie Mellon University

Research Intern | Summer 2016 | Pittsburgh, PA

Used high level synthesis (HLS) tools for implementing various machine learning algorithms on FPGAs.

AWARDS

- 2021 Rambus Fellowship in Electrical and Computer Engineering
- 2020 Analog Devices Outstanding Student Designer Award
- 2015 2nd place in the ACM LCPC and qualified for ACM ACPC (Regionals)
- 2013 Ranked 6th at the Lebanese Official Baccalaureate Exams