Opportunity Title: Machine Learning and Modelling of Complex Circuits to Provide Secure Hardware Assurance
Opportunity Reference Code: ICPD-2022-38

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2022-38

How to Apply

Create and release your Profile on Zintellect – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2022 6:00:00 PM Eastern Time Zone

Description

Research Topic Description, including Problem Statement:

With machine learning advances in hardware and software being powered by strong commercial interest and consumer awareness of data security/privacy it is becoming more practical to deploy trained models to the edge of a system on low power devices to filter information, make decisions and provide context to data before it is aggregated on back-end systems.

Neural networks are benefiting from advances in core principles, software libraries and optimized hardware to run them making an eco-system that is moving quickly but still relatively immature in terms of its success deploying solutions to “production”.

What threats and opportunities does using neural networks at the edge of a system present? i.e., how could somebody affect a system that has a neural network as a component, either to defeat, deceive or coerce the system?

Other thoughts for steer are:

- With the global diversity of electronic components and printed circuit board (PCB) manufacture and assembly supply chains, there is limited confidence that delivered assembled PCBs have been manufactured and assembled as designed without error. PCB testing is therefore required after manufacturing to verify the PCB functions as required and does not have component(s) missing, wrong component(s) added, component(s) that have failed or will

Opportunity Title: Machine Learning and Modelling of Complex Circuits to Provide Secure Hardware Assurance
Opportunity Reference Code: ICPD-2022-38

likely fail or components that are fake. Testing is a trade-off of how extensively to test the product versus time and cost to do the testing. Depending on the final PCB application the effort to assure the hardware in both secure and insecure environments can be considerable.

- Testing and fault finding on PCBs or finding components that are likely to suffer early failure is a difficult and time-consuming task to perform that does not scale with increasing PCB complexity. Added to this, when a PCB is assembled, measuring individual components values in circuit (e.g. a single resistor) is generally not a simple process without removing the component from the PCB first to measure its value. This is due to the other components on the same PCB net contributing to the in circuit measured value, not just that of the individual component in question.
- For example; the measured value of resistance of a PCB net will be the resultant combination of resistance of all components connected to that net. How could the circuit net be modelled to decompose the resultant value into the actual individual component values, with minimal knowledge of the circuit schematic and layout?
- Being able to quickly take probe measurements of PCB nets (e.g. resistance/capacitance/inductance) then running the results through a model to evaluate the individual components values would be of benefit to both the IC and wider industry allowing scalable and fast PCB testing and assurance. This would allow a rapid understanding of which components are out of tolerance, missing, fake or failed and would allow greater assurance PCBs without extensive and time-consuming testing

Example Approaches:

- Demonstrate on circuit nets of differing complexity
- Measure resistance, capacitance and inductive values of circuit nets with differing complexity.
- Model the component values and connections to agree with the measured values.
- Use machine learning and other approaches to invert the model and resultant measurements to evaluate the original component values.
- Add in additional known information to the evaluation, where necessary, (e.g. number of resistors/capacitors/inductors on the net) to determine the original components, aiming for minimal input to the model otherwise the more input required the less the approach can scale.
- Develop a verified modelling toolset that could be transferred over to the IC community upon completion of this postdoc.

Relevance to the Intelligence Community:

A concern of the Intelligence Community (IC) is in assuring the

Opportunity Title: Machine Learning and Modelling of Complex Circuits to Provide Secure Hardware Assurance
Opportunity Reference Code: ICPD-2022-38

provenance of hardware for critical and secure applications. With a global supply chain for PCB manufacture, how can a populated PCB be quickly assured that it has been manufactured as designed without fake, rejected or additional components add, whether this has been done maliciously or not? Using a quick probe test on each PCB net and decomposing the resultant values back to the individual component values would allow assurance that the components are as expected, and the PCB has not been tampered with or has had extra components added to the PCB that may degrade performance in critical IC applications.

Key Words: Machine Learning, Modelling, Electronics, Hardware Assurance, Printed Circuit Board, Fault Finding

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Academic Level(s):** Postdoctoral.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (2 👁)
  - **Computer, Information, and Data Sciences** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (27 👁)