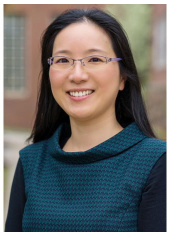
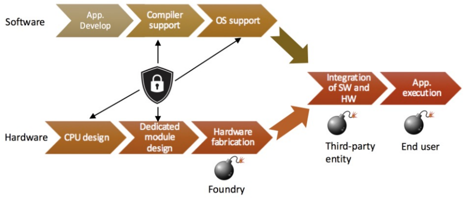
SaTC:CORE:Small: Towards Securing the Hardware and Software for Approximate Computing Systems

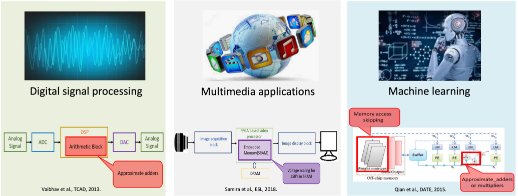


Qiaoyan Yu, University of New Hampshire

https://mypages.unh.edu/qyu/research

Motivation and Background





Vaibhav et al., TCAD, 2013.

Samira et al., ESL, 2018.

Qian et al., DATE, 2015.

Challenges

- Unique approximate behavior & computational uncertainty in approximate computing (AC) systems expose new attack opportunities.
- It is imperative to address the attacks from untrusted fabrication foundry, the 3rd-party entities for approximate SW and HW integration/testing, and the end user.

Scientific Impact

- Boundary-blurring introduces a new defense line to complement existing obfuscation methods
- New obfuscation methods facilitates to securely leverage AC mechanisms to lower power consumption and improve performance.

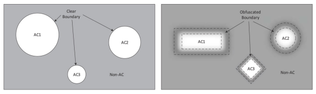
Key Contributions

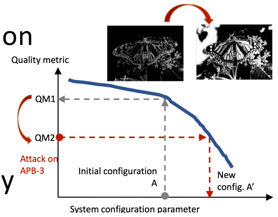
Develop holistic hardware-software integrated methods to secure AC systems

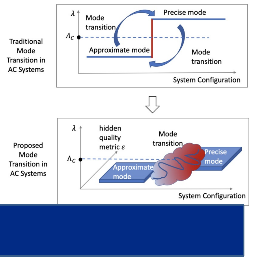
- Boundary-blurring obfuscation
- Non-linear Mixed-Boolean-Arithmetic transformation

$$x * y = (x \wedge \neg y) * (\neg x \wedge y) + (x \wedge y) * (x \vee y)$$

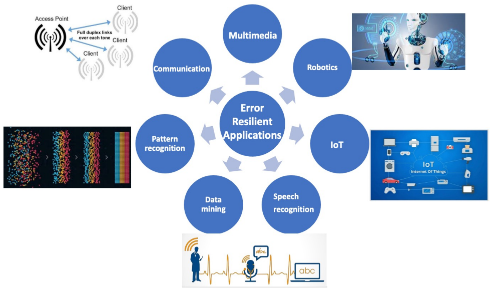
- White-Box cryptography: hide keys inside crypto function
- Context-switch detection: detect function boundary







Broader Impact



- Enable the secure usage of AC techniques in recognition, mining, and synthesis applications
- Supported two female Ph.D. students
- Promote undergraduate research via international cybersecurity competitions