Automatically Finding Hardware Vulnerabilities

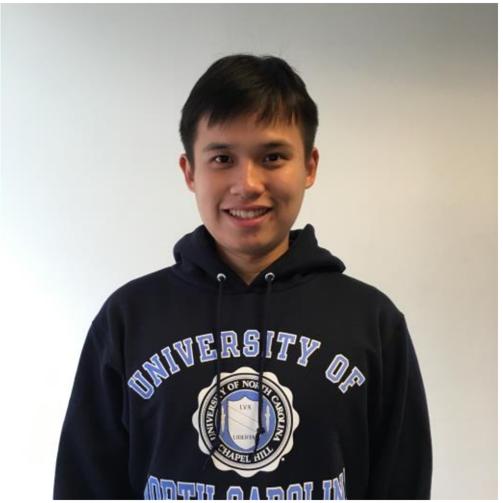
THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

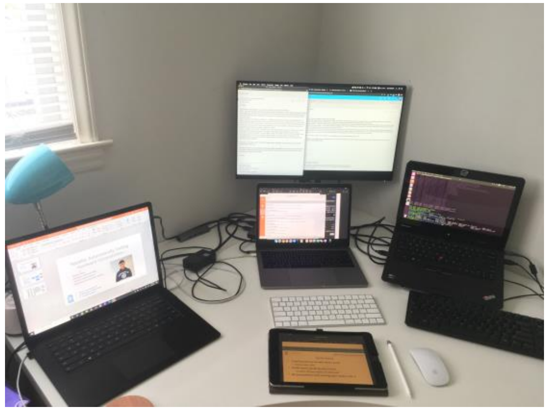
Martin Meng

Computer Science & Math

Advisor: Cynthia Sturton

Department of Computer Science

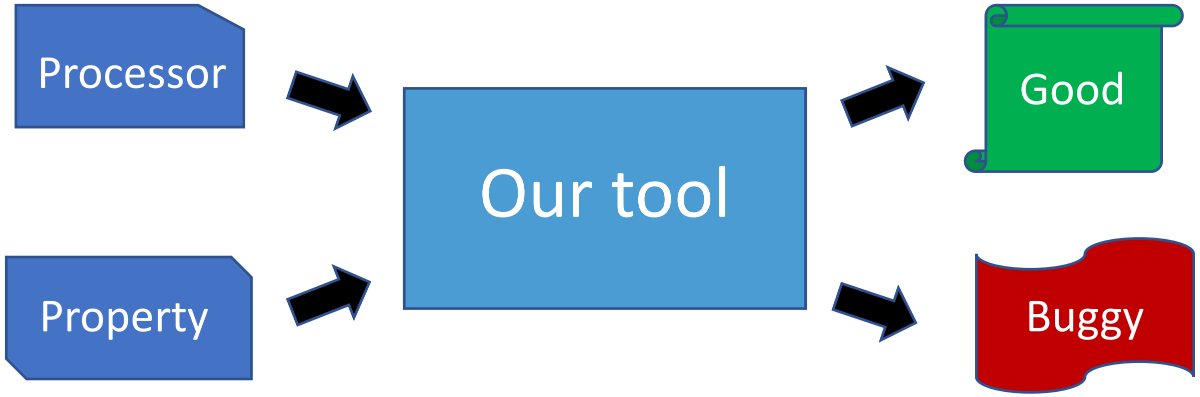




Research Question

Given security properties, how to efficiently find bugs in a processor design?

- Importance: finding bugs efficiently in a new processor can speed up the processor development cycle by saving time on the verification stage.
- Our tool: find all possible paths in 1 cycle of a processor design; stitch these paths to form a new path leading to a bug through a search algorithm.



Results

- Our tool can find deep bugs faster than best-known prior method.
- Hardware designers can save time by using our tool to verify their designs.
- Safer processors verified by our tool will be available to the world.

	Our tool	**Best-known prior method**
Shallow bugs	6.8 seconds	3.5 seconds
Deep bugs	8.3 seconds	> 4 hours

Table 1: an average-time comparison between our tool and the best-known prior method.