Hardware Trojan Detection via Chisel HDL

Compare different implementations of a component for the *PULPino* system

- Use techniques from fault tolerance for detecting hardware trojans.
- While we cannot use TLM/RTL models from others, we can create our own TLM/RTL models (using *SystemC*, *Verilog*, and/or *Chisel*) for components of the *PULPino* system.
- The output of these different implementations is given to a majority gate (i.e., use majority voting).
- Components that yield a different output from the majority of the components have hardware trojans.

Use the aforementioned software redundancy technique to determine which hardware component went bad, and when and how (i.e.., sequence of input patterns) did it go bad.

References (1)

- [Wikipedia contributors 2016] Wikipedia contributors, “Alice and Bob,” in *Wikipedia, The Free Encyclopedia: Cryptographic protocols*, Wikimedia Foundation, San Francisco, CA, February 28, 2018. Available online at: `https://en.wikipedia.org/wiki/Alice_and_Bob`; last accessed on October 26, 2016.
- [Khabarov 2015] Sergey Khabarov, answer to “What is meant by the FENCE instruction in the RISC-V instruction set?,” Stack Exchange Inc., New York, NY, November 23, 2015. Available online from *Stack Exchange Inc.: Stack Overflow: Questions* at: `https://stackoverflow.com/questions/26374435/what-is-meant-by-the-fence-instruction-in-the-risc-v-i` March 16, 2016 was the last accessed date.

References (2)

- [Bushnell 2000] Michael L. Bushnell and Vishwani D. Agrawal, “Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits,” in *Frontiers in Electronic Testing* series, Vol. 17, Springer Science+Business Media, Inc., New York, NY, 2000. DOI:10.1007/b117406.
- [Wang 2006] Laung-Terng Wang, Cheng-Wen Wu, and Xiaoqing Wen, “VLSI Test Principles And Architectures: Design for Testability,” in *The Morgan Kaufmann Series in Systems on Silicon*, Morgan Kaufmann, San Francisco, CA, 2006.