SAND2019-8026D

The Center for Cyber Defenders

Expanding computer security knowledge

Velocity

Gate-Level Fault Testing of Synthesizable RISC-V Processors

Meryl Flaherty, Texas Tech University

Project Mentor: T.J. Mannos, Org. 5253

Problem Statement:

- Test safety and security critical software on hardware without fault mitigations at the gate level by emulating the hardware on FPGA and ASIC devices.

Objectives and Approach:

- Inject faults to individual gates using saboteur circuits accessible by scan chain
- Test four types of faults: stuck-at-0, stuck-at-1, invert, and delay
- Create fault-testing platform for synthesizable processors, modeled in Scala-based Chisel hardware description language and placed on Xilinx VC707 FPGA development board
- Run AES256 encryption program and check expected output with actual output
- Port hardware implementation from Xilinx VC707 to ZCU102 FPGA development board

```
 moving .text from 0x00001460 to 0x40000000
 moving .data from 0x00007d30 to 0x400068d0
txt:
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

key:
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
---
enc:
8E A2 B7 CA 51 67 45 BF EA FC 49 90 4B 49 60 89

tst:
8E A2 B7 CA 51 67 45 BF EA FC 49 90 4B 49 60 89

Match
```

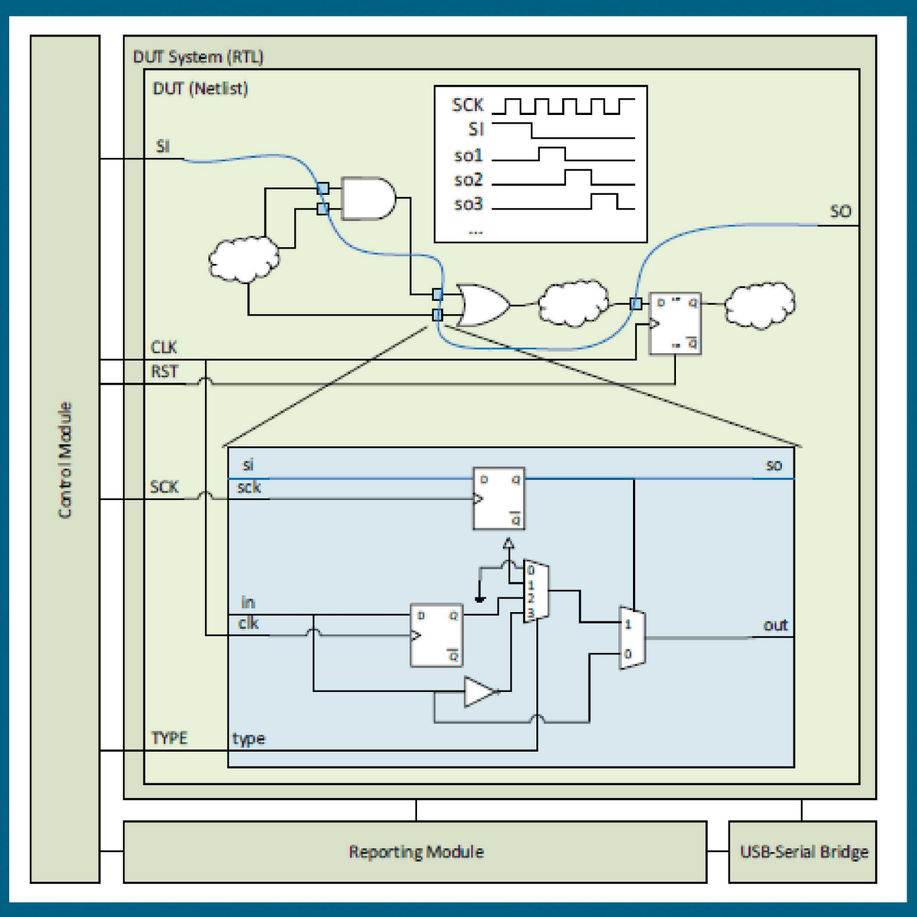
Example output of AES256 program on serial port.

Results

- Testing time for 335,834 fault points on RISC-V processor reduced from 4.5 years to 30 hours

Impact and Benefits:

- Scalability for testing increasingly complex processors where gate-level simulation is prohibitive
- Discover how various faults cause different software failure (faulty output, leaked plaintext or key, etc.)
- Allow engineers to make better design decisions with rapid testing of fault mitigations
- Reduced hardware cost by implementing on FPGAs rather than ASIC macros



Device under test with saboteur circuits (blue) added to gate inputs.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.