Automation for Side-Channel and Security Testing of Hardware IP

Niels Samwel (niels.samwel@pqshield.com)
Side-Channel and Security Testing Infrastructure

Post Quantum Cryptography Development

- Quality Testing
- Side-Channel Testing
- Fuzzing
- Future
  - Side-Channel Simulation
  - Fault Simulation
Side-Channel Setup

- **Target**
  - Chipwhisperer CW305
    - Artix 7 FPGA
- **Oscilloscope**
  - Picoscope 6424E
    - 8 bit resolution (can be increased to 12-bit)
    - 500 MHz bandwidth
    - 4 GS memory
Side-Channel Testing (FIPS 140-3)

- 9 Side-Channel Setups
- Challenges
  - Fully remote company
  - Number of tests
Side-Channel Testing (Common Criteria)

TVLA Limitations

- Univariate tests
- No estimation of actual security

Ad Hoc Testing

- Goal: estimate number of traces for key recovery
- Target specific vulnerabilities
- Attack types
  - Template attacks
  - Key recovery attacks
  - CPA/DPA

Diagram:

- Oxford
- SCA Lab: sca1, sca2, sca3
- Fast Storage Server
- esDynamic Server
- Data Center
- 10Gb/s
Product Quality Testing

Hardware

- Design Phase
  - Linting (VC Spyglass)
  - Physical design implementation
  - Automated FPGA functional testing
  - Peer review each commit
- Verification Phase
  - Constraint random verification (UVM)
  - Condition/Toggle coverage
  - Bounded model checking (VC Formal)
- Dashboards with metrics

Software

- Implementation Phase
  - Static analysis
  - Automated FPGA functional testing
  - Peer review each commit
- Verification Phase
  - System level tests
  - Integration tests
  - Functional tests
  - Unit tests
  - Coverage testing
  - Fuzzing
## PQShield’s Security Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Target</th>
<th>FIPS 140-3 level</th>
<th>Common-Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Safe against fuzzing Safe against remote attacks*</td>
<td>Level 1</td>
<td>EAL1 AVA_VAN.1</td>
</tr>
<tr>
<td>1</td>
<td>Safe against “push button” physical attacks (basic attack potential)</td>
<td>SW: Level 2 HW: Level 3</td>
<td>EAL2 to 3 AVA_VAN.2</td>
</tr>
<tr>
<td>2</td>
<td>Safe against expert lab (high attack potential)</td>
<td>SW: Level 2 HW: Level 4</td>
<td>EAL4+ to 7 AVA_VAN.5</td>
</tr>
</tbody>
</table>

*For software libraries, micro-architectural attacks such as RowHammer, Spectre, Meltdown... may be applicable if the hardware platform is vulnerable to them.