Detecting Power Attacks on Reconfigurable Hardware

Adrien Le Masle    Wayne Luk

Department of Computing
Imperial College London, UK

22nd International Conference on Field Programmable Logic and Applications
Main Contributions

- General framework to detect insertion of power measurement circuit in device’s power rail
  - ring oscillator-based power monitor circuit monitors supply voltage variations
  - attack detector circuit implements power attack detection strategy
  - abnormal supply voltages and power rail resistance values detected

- Implementation of framework
  - 3300 LUTs on Spartan-6 LX45 FPGA
  - insertion of 1Ω shunt resistor and high supply voltage detected on AES and RSA crypto-system @ 20 MHz
  - no false-positive and false-negative for proper operating margins
Outline

1 Introduction
   - Background
   - Problem
   - Main Contributions

2 Power Attack Detection Framework
   - Framework
   - Power Monitor
   - Attack Detector

3 Results
   - Experimental Setting
   - Detection Rate

4 Conclusion
   - Future Work
   - Summary
Outline

1 Introduction
   - Background
   - Problem
   - Main Contributions

2 Power Attack Detection Framework
   - Framework
   - Power Monitor
   - Attack Detector

3 Results
   - Experimental Setting
   - Detection Rate

4 Conclusion
   - Future Work
   - Summary
Security of encryption algorithm implementation

- Encryption algorithm
  - brute-force attack or exhaustive key search computationally infeasible
  - resists cryptanalysis

- Physical implementation of algorithm
  - leaks information
  - creates security flaws

- Side-channel attacks exploit these physical flaws
Power attacks

- Transistor switching inside device
  - leaks information about computation
  - power easily measured inserting shunt resistor in main power rail

- Simple Power Analysis (SPA)
  - direct information about encryption key through single power trace
  - eg: multiplication/squaring in RSA modular exponentiation

- Differential Power Analysis (DPA) [1]
  - information from multiple power traces with statistical methods
  - eg: DPA against AES or DES

- Successfully demonstrated on private and public key encryptions

FPGA power measurement

\[ P = V_{\text{INT}} I = \left( V_{\text{CCINT}} - \left( V_{\text{EXT}} + V_{\text{NET}} \right) \right) I \approx V_{\text{CCINT}} I \]

\[ I = \frac{V_{\text{EXT}}}{R_{\text{EXT}}} \]

- Variations of \( R_{\text{EXT}} \) create variations of supply voltage \( V_{\text{INT}} \)
### Problem

- **Two types of countermeasures**
  - **masking**: randomize intermediate values processed by device [2]
    - application-dependent
    - 2-3 times area overhead
  - **hiding**: remove data dependency of power consumption [3,4]
    - eg: differential logic, symmetrical routing
    - 3-10 times area overhead
    - slow

- **Challenge**
  - preventing power attacks area-consuming and slows down design
  - many countermeasures often need to be combined
  - can’t we simply detect power attacks?

---

[2] F. Regazzoni et al., *FPGA implementations of the AES masked against power analysis attacks*, COSADE 2011
[3] K. Tiri et al., *A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation*, DATE ‘04
Main Contributions

- General framework to detect insertion of power measurement circuit in device’s power rail
  - ring oscillator-based power monitor circuit monitors supply voltage variations
  - attack detector circuit implements power attack detection strategy
  - abnormal supply voltages and power rail resistance values detected

- Implementation of framework
  - 3300 LUTs on Spartan-6 LX45 FPGA
  - insertion of 1Ω shunt resistor and high supply voltage detected on AES and RSA crypto-system @ 20 MHz
  - no false-positive and false-negative for proper operating margins
Outline

1. Introduction
   - Background
   - Problem
   - Main Contributions

2. Power Attack Detection Framework
   - Framework
   - Power Monitor
   - Attack Detector

3. Results
   - Experimental Setting
   - Detection Rate

4. Conclusion
   - Future Work
   - Summary
### Hardware cores
- Cryptographic functions (RSA, AES, RNG, ...)
- Non-critical tasks (communication, clock generation, ...)

### Power monitor
- Measures FPGA supply voltage variations on-chip

### Attack detector
- Receives information about state of core’s power consumption
- Checks whether power consumption stays in pre-defined range

---

A. Le Masle and W. Luk (Department of Computing, Imperial College London, UK)

Detecting Power Attacks on Reconfigurable Hardware

FPL 2012
Oscillation frequency of ring oscillator affected by supply voltage

\[ f_R \approx k_0 V_{\text{INT}} + f_0 \]

High resolution needs accumulation of many oscillations

- measurement period \( \uparrow \), response time \( \downarrow \)
- solution: evenly distribute network of ROs across chip and accumulate oscillations count \( \rightarrow \) placement and routing constraints
- better resolution, more consistent measurement
Advantages of ring oscillators

- built with primitives available to all commercial FPGAs
- relatively small and easily uniformly distributed across the chip
- ring oscillator’s frequency scales with advances in fabrication technology

Higher sampling rate than current FPGAs ADCs

- Virtex-6 ADC: 200 kHz
- ring oscillator-based power monitor: < 8 MHz
All possible input values cannot be tested

- for each core $i$, $p_{\text{ref}}, p_{\text{min},i}$ and $\Delta p_{\text{ref},i}$ are approximations

Margins $m_{\text{ref}}$ and $m_{\text{ref},i}$ on $p_{\text{ref}}$ and $\Delta p_{\text{ref},i}$

\[
p^*_{\text{ref}} = p_{\text{ref}}(1 + m_{\text{ref}})
\]

\[
\Delta p^*_{\text{ref},i} = (p^*_{\text{ref}} - p_{\text{min},i})(1 + m_{\text{ref},i})
\]
Monitoring (1/2)

- \( p(t) \) instantaneous power monitor reading

\[
\Delta p(t) = p_{\text{ref}}^* - p(t) \\
p_{\text{min}}(t) = p_{\text{ref}}^* - \sum_{i \in S(t)} \Delta p_{\text{ref},i}^*
\]

- At time \( t \), subset \( S(t) \) of \( n \) hardware cores are running

- Attack flag raised if

\[
p(t) > p_{\text{ref}}^* \quad \text{or} \quad \Delta p(t) > \sum_{i \in S(t)} \Delta p_{\text{ref},i}^*
\]
Normal operating conditions
- power trace $p(t)$ between $p_{\text{ref}}^*$ and $p_{\text{min}}(t)$

Supply voltage too high
- $p$ raises over $p_{\text{ref}}^*$ → detected by equation 1

Supply voltage too low or power rail resistance too high
- $p$ falls below $p_{\text{min}}$ at time $t_d$ → detected by equation 2
Outline

1 Introduction
   • Background
   • Problem
   • Main Contributions

2 Power Attack Detection Framework
   • Framework
   • Power Monitor
   • Attack Detector

3 Results
   • Experimental Setting
   • Detection Rate

4 Conclusion
   • Future Work
   • Summary
Experimental Setting

- Modified Pico E-101 board with Spartan-6 LX45 FPGA
- Switching regulators replaced by low dropout regulators
- 1.2V rail: output capacitors removed, 1Ω shunt resistor inserted
- Voltage drop across resistor measured with Tektronix MSO 2024 200 MHz oscilloscope through SMA connector
Case Study

- Crypto-system with 5 main cores @ 20 MHz
  - detection logic, 512-bit RSA, 128-bit AES, Microblaze and UART

- Three tests cases
  - RSA encryption
  - AES encryption
  - RSA and AES encryptions in parallel

- Three operating conditions
  - original board
  - modified board with higher supply voltage $V_{\text{INT}} = 1.25\,V$
  - modified board with shunt resistor $R_{\text{EXT}} = 1\,\Omega$
Parameters

- Power monitor
  - 144 ring oscillators @ 350 MHz
  - power monitor reading updated @ 8 MHz

- RSA/AES cores calibrated with 100/1000 random input pairs on original board

- Power consumption of Microblaze and UART neglected
  - UART never runs in parallel with RSA or AES
  - Microblaze only waits for interrupt

- Power monitor and attack detector area consumption
  - 3300 LUTs
  - 12% of area available on Spartan-6 LX45
Detected attacks (% of total runs - of which % of high voltage detections)

<table>
<thead>
<tr>
<th></th>
<th>$p_{\text{ref}}$</th>
<th>$p_{\text{ref}} + 1%$</th>
<th>$p_{\text{ref}} + 5%$</th>
<th>$\Delta p_{\text{ref},i}$</th>
<th>$\Delta p_{\text{ref},i} + 10%$</th>
<th>$\Delta p_{\text{ref},i} + 50%$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RSA</strong></td>
<td>Original</td>
<td>3.8 - 100</td>
<td>0 - NA</td>
<td>0 - NA</td>
<td>98.6 - 0</td>
<td>0 - NA</td>
</tr>
<tr>
<td></td>
<td>$V_{\text{INT}} = 1.25\text{V}$</td>
<td>100 - 100</td>
<td>100 - 100</td>
<td>0 - NA</td>
<td>100 - 100</td>
<td>100 - 100</td>
</tr>
<tr>
<td></td>
<td>$R_{\text{EXT}} = 1\Omega$</td>
<td>0.001 - 100</td>
<td>0.001 - 100</td>
<td>0 - NA</td>
<td>100 - 0</td>
<td>100 - 0.004</td>
</tr>
<tr>
<td><strong>AES</strong></td>
<td>Original</td>
<td>0.11 - 100</td>
<td>0 - NA</td>
<td>0 - NA</td>
<td>1.6 - 0</td>
<td>0 - NA</td>
</tr>
<tr>
<td></td>
<td>$V_{\text{INT}} = 1.25\text{V}$</td>
<td>100 - 100</td>
<td>100 - 100</td>
<td>0.13 - 100</td>
<td>100 - 100</td>
<td>100 - 100</td>
</tr>
<tr>
<td></td>
<td>$R_{\text{EXT}} = 1\Omega$</td>
<td>0.001 - 100</td>
<td>0.001 - 100</td>
<td>0 - NA</td>
<td>100 - 0.004</td>
<td>100 - 0.004</td>
</tr>
<tr>
<td><strong>RSA+AES</strong></td>
<td>Original</td>
<td>1.8 - 100</td>
<td>0 - NA</td>
<td>0 - NA</td>
<td>2.7 - 0</td>
<td>0 - NA</td>
</tr>
<tr>
<td></td>
<td>$V_{\text{INT}} = 1.25\text{V}$</td>
<td>100 - 100</td>
<td>100 - 100</td>
<td>0.02 - 100</td>
<td>100 - 100</td>
<td>100 - 100</td>
</tr>
<tr>
<td></td>
<td>$R_{\text{EXT}} = 1\Omega$</td>
<td>0.001 - 100</td>
<td>0.001 - 100</td>
<td>0 - NA</td>
<td>100 - 0.02</td>
<td>100 - 0.02</td>
</tr>
</tbody>
</table>

- **High voltage detection (equation 1)**
  - no margin $m_{\text{ref}}$ on $p_{\text{ref}}$ → false-positives up to 3.8%
  - margin $m_{\text{ref}} = 1\%$ → no false-positives/false-negatives
  - margin greater than 5% → false-negatives up to 99%

- **Shunt resistor detection (equation 2) for $m_{\text{ref}} = 1\%$**
  - no margin $m_{\text{ref},i}$ on $\Delta p_{\text{ref},i}$ → false-positives up to 98.6%
  - margin $m_{\text{ref},i} = 10\%$ → no false-positives/false-negatives
  - margin $m_{\text{ref},i}$ greater than 50% → false-negatives appear (0.3%)
Outline

1. Introduction
   - Background
   - Problem
   - Main Contributions

2. Power Attack Detection Framework
   - Framework
   - Power Monitor
   - Attack Detector

3. Results
   - Experimental Setting
   - Detection Rate

4. Conclusion
   - Future Work
   - Summary
Future Work

- Evaluate attack detector for lower shunt resistor values
- Confirm temperature variations have only a negligible effect on attack detection
- Take into account power consumption of individual instructions of processor cores
- Investigate other on-chip measurement methods
- Explore attack detection of electromagnetic attacks
General framework to detect insertion of power measurement circuit in device’s power rail

- Ring oscillator-based power monitor circuit monitors supply voltage variations
- Attack detector circuit implements power attack detection strategy
- Abnormal supply voltages and power rail resistance values detected

Implementation of framework on Spartan-6 LX45 FPGA

- 3300 LUTs, 12% of total area available
- Insertion of 1Ω shunt resistor and high supply voltage detected on AES and RSA crypto-system @ 20 MHz
- No false-positive and false-negative for proper operating margins