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

Outline

Security of encryption algorithm implementation

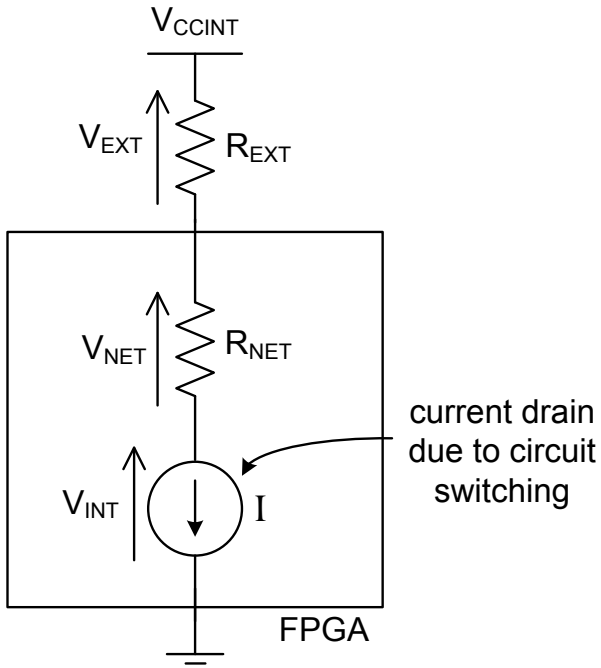
- Encryption algorithm
  - brute-force attack or exhaustive key search computationally infeasible
  - resists cryptanalysis
- Physical implementation of algorithm
  - leaks information
  - creates security flaws
- Side-channel attacks exploit these physical flaws

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

[1] P. Kocher et al., *Differential power analysis*, CRYPTO '99

FPGA power measurement



$$P = V_{INT} I = (V_{CCINT} - (V_{EXT} + V_{NET}))I \approx V_{CCINT} I$$
$$I = V_{EXT} / R_{EXT}$$

- Variations of R_{EXT} create variations of supply voltage V_{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

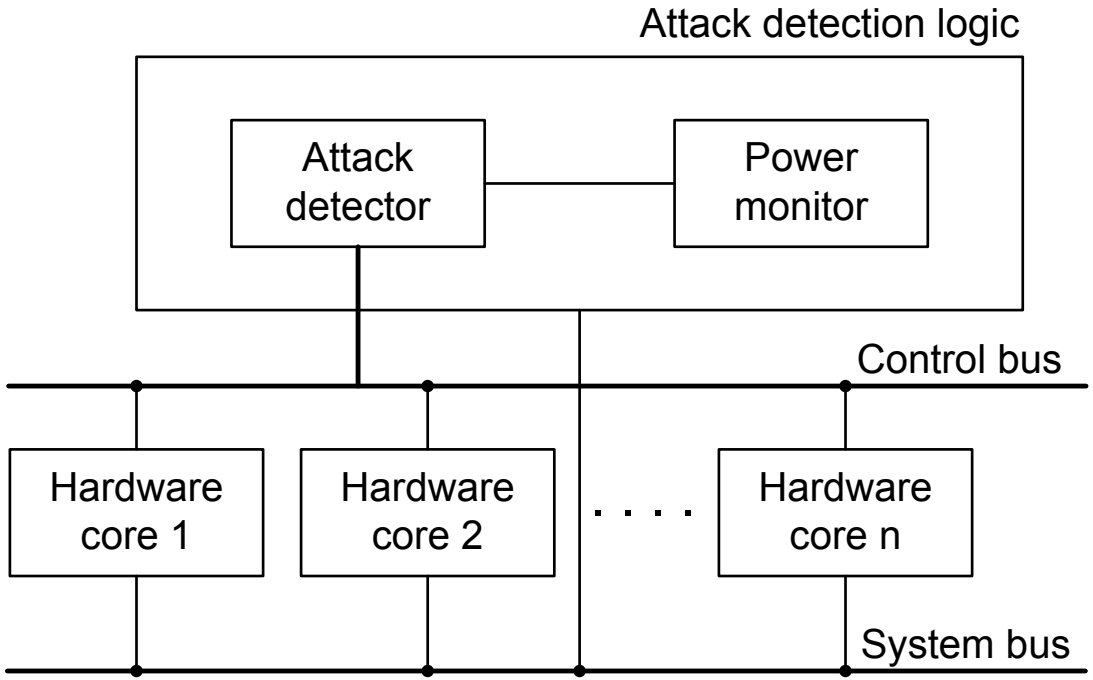
[4] P. Yu et al., *Secure FPGA circuits using controlled placement and routing*, CODES+ISSS '07

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

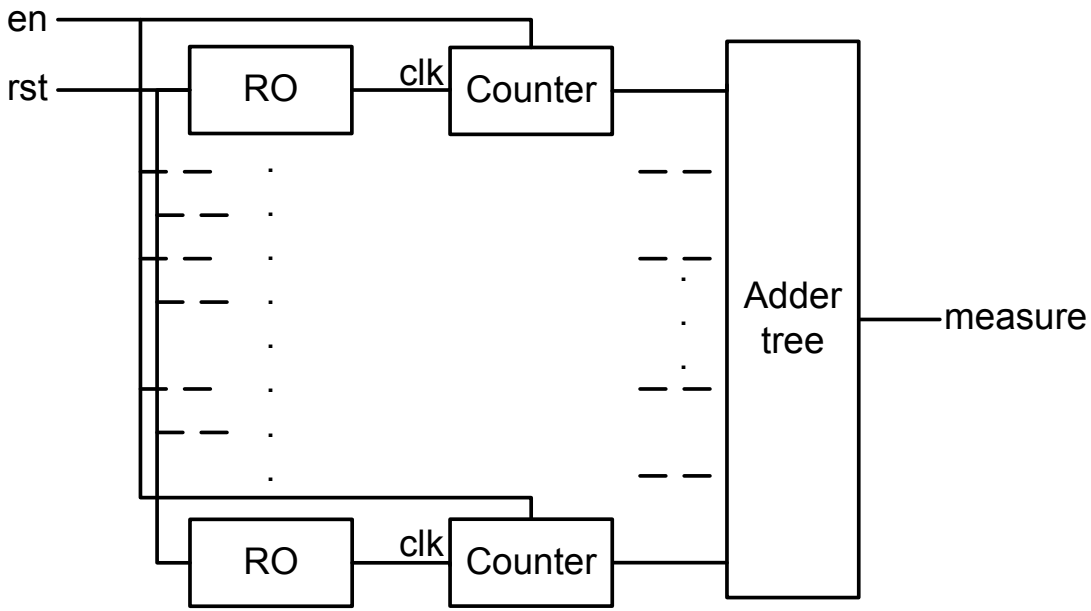
Outline

Framework



- 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

Power Monitor (1/2)



- Oscillation frequency of ring oscillator affected by supply voltage

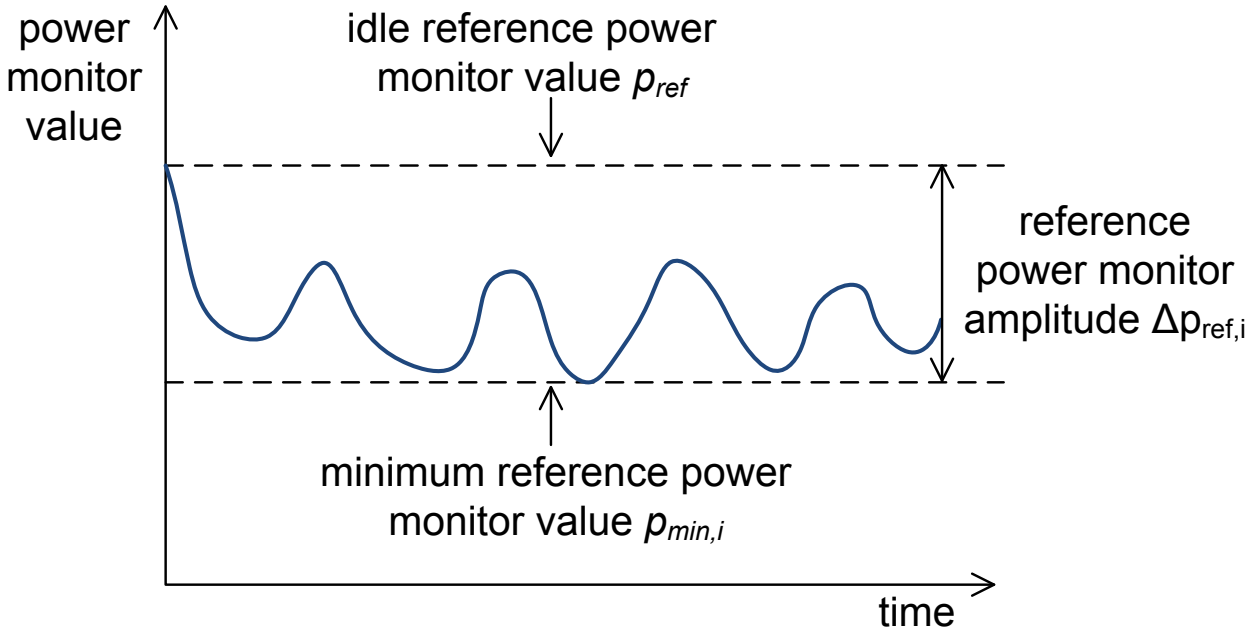
$$f_R \approx k_0 V_{INT} + f_0$$

- High resolution needs accumulation of many oscillations
  - measurement period ↗, response time ↘
  - solution: evenly distribute network of ROs across chip and accumulate oscillations count → placement and routing constraints
  - better resolution, more consistent measurement

Power Monitor (2/2)

- 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

Calibration



- All possible input values cannot be tested
  - for each core i, p_{ref}, $p_{min,i}$ and$\Delta p_{ref,i}$ are approximations
- Margins m_{ref} and $m_{ref,i}$ on p_{ref} and $\Delta p_{ref,i}$

$$p^*_{ref} = p_{ref}(1 + m_{ref})$$
$$\Delta p^*_{ref,i} = (p^*_{ref} - p_{min,i})(1 + m_{ref,i})$$

Monitoring (1/2)

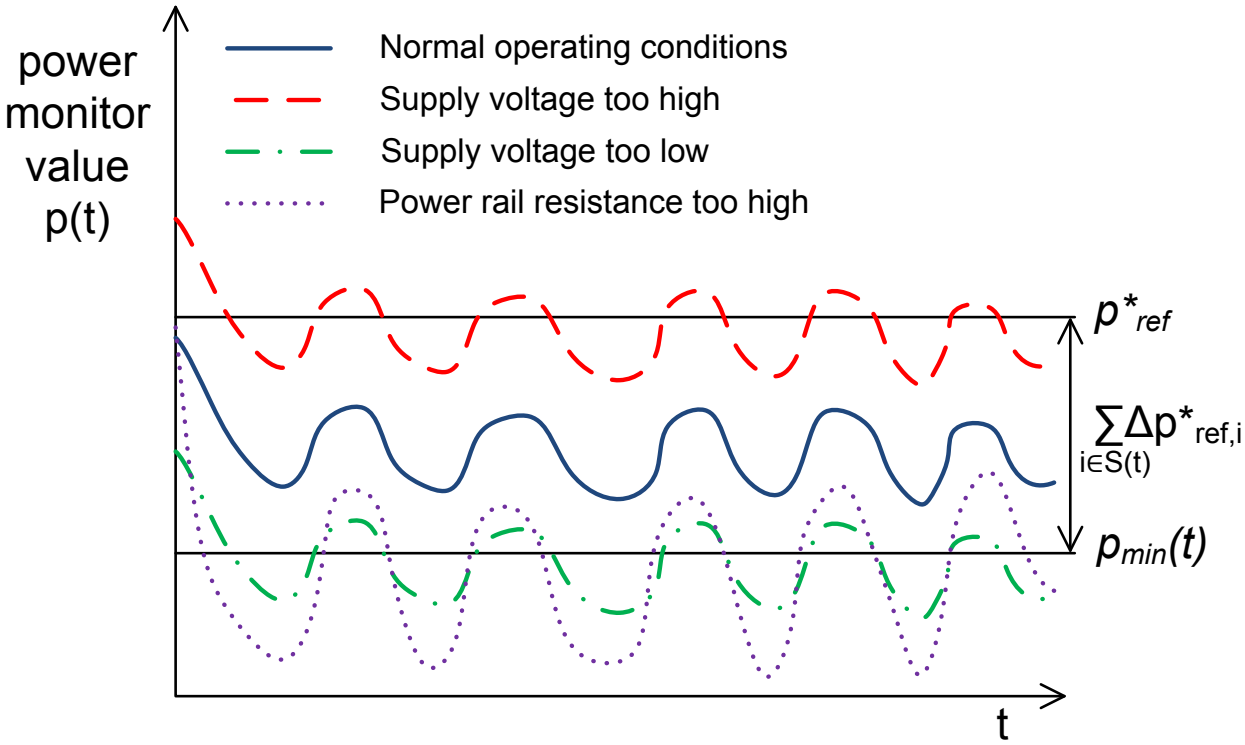
- $p(t)$ instantaneous power monitor reading

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

- At time t, subset $S(t)$ of n hardware cores are running
- Attack flag raised if

$$p(t) > p^*_{ref} \text{ or} \quad (1)$$
$$\Delta p(t) > \sum_{i \in S(t)} \Delta p^*_{ref,i} \quad (2)$$

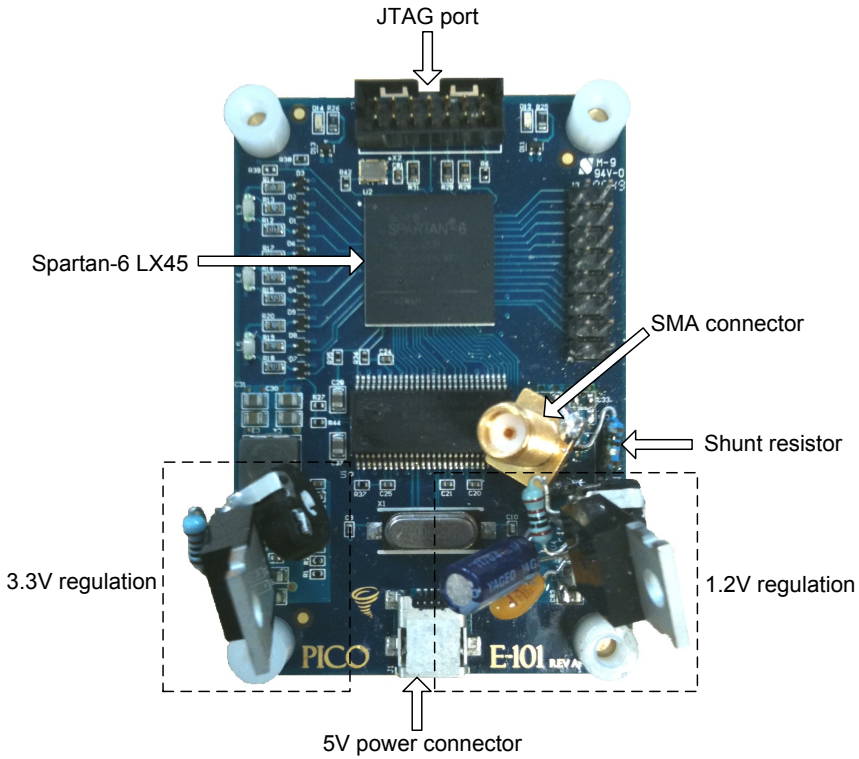
Monitoring (2/2)



- Normal operating conditions
  - power trace $p(t)$ between p^*_{ref} and $p_{min}(t)$
- Supply voltage too high
  - p raises over $p^*_{ref} \rightarrow$ detected by equation 1
- Supply voltage too low or power rail resistance too high
  - p falls below p_{min} at time $t_d \rightarrow$ detected by equation 2

Outline

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 $V_{INT} = 1.25V$
  - modified board with shunt resistor $R_{EXT} = 1\ \Omega$

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

Detection Rate

Detected attacks (% of total runs - of which % of high voltage detections)

		p_{ref}	$p_{ref} + 1\%$	$p_{ref} + 5\%$	$\Delta p_{ref,i}$	$\Delta p_{ref,i} + 10\%$	$\Delta p_{ref,i} + 50\%$
RSA	Original	3.8 - 100	0 - NA	0 - NA	98.6 - 0	0 - NA	0 - NA
	$V_{INT} = 1.25V$	100 - 100	100 - 100	0 - NA	100 - 100	100 - 100	100 - 100
	$R_{EXT} = 1\Omega$	0.001 - 100	0.001 - 100	0 - NA	100 - 0	100 - 0.004	100 - 0.006
AES	Original	0.11 - 100	0 - NA	0 - NA	1.6 - 0	0 - NA	0 - NA
	$V_{INT} = 1.25V$	100 - 100	100 - 100	0.13 - 100	100 - 100	100 - 100	100 - 100
	$R_{EXT} = 1\Omega$	0.001 - 100	0.001 - 100	0 - NA	100 - 0.004	100 - 0.004	99.7 - 0.004
RSA+AES	Original	1.8 - 100	0 - NA	0 - NA	2.7 - 0	0 - NA	0 - NA
	$V_{INT} = 1.25V$	100 - 100	100 - 100	0.02 - 100	100 - 100	100 - 100	100 - 100
	$R_{EXT} = 1\Omega$	0.001 - 100	0.001 - 100	0 - NA	100 - 0.02	100 - 0.02	100 - 0.003

- High voltage detection (equation 1)
  - no margin m_{ref} on p_{ref} $\rightarrow$ false-positives up to 3.8%
  - margin $m_{ref} = 1\%$ $\rightarrow$ no false-positives/false-negatives
  - margin greater than 5% $\rightarrow$ false-negatives up to 99%
- Shunt resistor detection (equation 2) for $m_{ref} = 1\%$
  - no margin $m_{ref,i}$ on $\Delta p_{ref,i}$ $\rightarrow$ false-positives up to 98.6%
  - margin $m_{ref,i} = 10\%$ $\rightarrow$ no false-positives/false-negatives
  - margin $m_{ref,i}$ greater than 50% $\rightarrow$ false-negatives appear (0.3%)

Outline

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

Summary

- 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