Differential Power Analysis (DPA)

- Kocher et al.\(^1\) introduced DPA that measures power consumption of a device to reveal secret information.

Attack Scheme

\[
\begin{pmatrix}
t_{1,1} & t_{1,2} & \ldots & t_{1,T} \\
t_{2,1} & t_{2,2} & \ldots & t_{2,T} \\
\vdots & \vdots & \ddots & \vdots \\
t_{N,1} & t_{N,2} & \ldots & t_{N,T}
\end{pmatrix}
\]

Figure 1: Correlating hypothetical power with measured power traces
**Attack Scheme**

\[
\begin{pmatrix}
h_{1,1} & h_{1,2} & \ldots & h_{1,K} \\
h_{2,1} & h_{2,2} & \ldots & h_{2,K} \\
:\vdots & \vdots & \ddots & \vdots \\
h_{N,1} & h_{N,2} & \ldots & h_{N,K}
\end{pmatrix}
\begin{pmatrix}
t_{1,1} & t_{1,2} & \ldots & t_{1,T} \\
t_{2,1} & t_{2,2} & \ldots & t_{2,T} \\
:\vdots & \vdots & \ddots & \vdots \\
t_{N,1} & t_{N,2} & \ldots & t_{N,T}
\end{pmatrix}
\]

Figure 2: Correlating hypothetical power with measured power traces
Result of DPA on AES-128 Encryption

First byte of the key = 19
Motivation

Can we identify the processor components which causes leakage?
Motivation

Can we identify the processor components which causes leakage?

Step 1: Power patterns need to be identified

Step 2: Quantify the leakage

Step 3: Pinpointing the source of leakage
Total power = Static power + Dynamic power

Figure 3: Power consumption in CMOS circuit
Capturing Power Patterns

Figure 4: Hamming-distance model
Quantifying Leakage

Side-channel Vulnerability Factor (SVF)$^2$

---

Setup

- Target Processor: SHAKTI C-Class\(^3\)

- 64 bit, 6-stage pipeline which supports RISC-V ISA

- Benchmark program: AES-128 encryption compiled using riscv-gcc\(^4\) compiler version 5.4.0

---


Methodology

- Formation of HD Matrix
- Feature Analysis
- Correlation Analysis
Formation of HD Matrix

- Value Change Dump (VCD) files are collected for \( n \) samples

Figure 5: Formation of HD matrix from data matrix
Feature Analysis

- Every feature of HD matrix (Side-channel) is correlated with HD vector of actual data (oracle) using Pearson’s correlation coefficient.

- Features having high correlation are selected for further analysis.
Correlation Analysis

Figure 6: Leakage analysis of a module
Results

Figure 7: Leakages during AES-SubBytes operation in SHAKTI C-Class components
Results

Figure 8: Leakages during AES-MixColumns operation in SHAKTI C-Class components
Figure 9: Leakages found in FPU module after $1^{st}$ round SubByte operation
# Expected and Unexpected Leakage

## Expected Modules that Leak
- ✓ Data Cache
- ✓ Register File
- ✓ ALU
- ✓ Pipeline Buffers

## Unexpected Modules that Leak
- ✓ Floating Point Unit
- ✓ Instruction Memory
- ✓ Branch Prediction Unit
Unexpected Leakage Analysis

- \text{ff\_input\$D\_IN[211:0]} signal in FPU leaks data from register file.

- \text{Maybe}\# construct in Bluespec System Verilog leaks data though the validating condition fail. Adding control bits(0/1) with data and passing it
Work In Progress

- Adding Side-channel countermeasures for leaking modules such as dcache, fpu, imem, bpu etc

- In order to improve Side-channel security of the system, adding power analysis validations at the development stage

- Validate the device against public key ciphers such as RSA, ECC
Thank you
Any Questions…?