Side-Channel Analysis
- A physical-level perspective

Lang Lin
Who am I

• 5\textsuperscript{th} year PhD candidate in ECE

• Advisor: Professor Wayne Burleson

• Circuit design, RFID & hardware security
Outline

• Introduction
• Differential Power Analysis Attack
• Countermeasures
• Research overview
• Conclusions
Outline

• Introduction
• Differential Power Analysis Attack
• Countermeasures
• Research overview
• Conclusions
Physical Implementation Attacks

- Cryptology = Cryptography + Cryptanalysis
  - Cryptography: the strength of mathematics
  - Cryptanalysis: there must be weakness!
- Physical implementation attack
  - Crypto algorithms on silicon are not that secure
  - Implementation dependent, technology dependent
  - Logic function is the same, but physical property is different
Physical Implementation Attacks

- Cryptology = Cryptography + Cryptanalysis
  - Cryptography: the strength of mathematics
  - Cryptanalysis: there must be weakness!
- Physical implementation attack
  - Crypto algorithms on silicon are not that secure
  - Implementation dependent, technology dependent
  - Logic function is the same, but physical property is different

\[
A + B = ?
\]
Side-Channel Analysis Attacks

- SCA Attacks: physical implementation (both circuit level and architecture level) of crypto circuits can leak secret information to the adversary
Power Analysis Attack

“Computing, like all processes proceeding at a finite rate, must involve some dissipation.”

Rolf William Landauer

- Power Analysis Attack: measure and analyze the data-dependent power traces to extract secret digital information
  - Simple Power Analysis (SPA): “a one-to-one mapping”
  - Differential Power Analysis (DPA): binary grouping
  - Correlation Power Analysis (CPA): linear analysis
  - High-order DPA
  - Template attack: build the power model on-the-fly

Measured traces of the power supply current showing how the power is correlated with the logic values.
Crypto Circuit Implementation

- CMOS technology
  - Complementary metal–oxide–semiconductor
  - PMOS and NMOS
  - Basic elements to construct memories, microcontrollers and many digital/analog circuits

\[ F = \overline{G} \]

PUN and PDN are Dual Networks

CMOS inverter: \( Q = \sim A \)
Power dependence on data

- Method: Give all possible input patterns to a CMOS logic gate and measure power consumption
- Coefficient of variation (CV): a normalized measure of power dependence on input patterns

Example of data-dependent power across CMOS technologies: CMOS 2-input NAND gate
Outline

• Introduction
• Differential Power Analysis Attack
• Countermeasures
• Research overview
• Conclusions
DPA attack

• Before attacking the secret key:
  – Have the targeting device and know the power model
  – Know the type of crypto algorithm
  – Know the plaintext (or ciphertext)
  – Can measure the power traces
Whiteboard exercise: a naïve DPA

- **Goal**: extract the secret 3-bit key
- **Assumptions of the implementation:**
  - The dynamic power of the output bus dominates
  - Implemented with CMOS combinational logic

Plaintexts:

- 010
- 011
- 101
- 010
- 101

Secret key XXX

Power traces on the scope
Procedure of DPA attack

1. Give known plaintexts
2. Measure power traces
Procedure of DPA attack

1. Give known plaintexts
2. Measure power traces
3. Create a power profile

[Diagram showing the procedure with waveforms and data points]
Procedure of DPA attack

Give known plaintexts

Measure power traces

Create a power profile

Generate differential power curves (DPCs):
1. Make a key guess
2. Use a selection function (e.g. b2) to group the power traces
3. Add and subtract
4. Try all keys to get all DPCs

\[ \begin{align*}
100101 & \quad 110011 & \quad 000000 & \quad 111110 & \cdots \\
\text{b2=0} & \quad \text{b2=1} & \quad \text{b2=0} & \quad \text{b2=1} \\
\vdots & \quad \vdots & \quad \vdots & \quad \vdots \\
\end{align*} \]
Procedure of DPA attack

1. Give known plaintexts
2. Measure power traces
3. Create a power profile
4. Generate differential power curves (DPCs):
   1. Make a key guess
   2. Use a selection function (e.g. b2) to group the power traces
   3. Add and subtract
   4. Try all keys to get all DPCs
5. Extract the key by a peak on the DPCs?
   - YES: Report the number of power traces
   - NO: Repeat steps 1-4
DPCs

- Attacking AES substitution box (8-bit secret key k0..k7) implemented on FPGA
- Correct key guess: a peak shows up!
- Number of power traces analyzed VS secret key extraction
Outline

• Introduction
• Differential Power Analysis Attack
• Countermeasures
• Research overview
• Conclusions
Prevent side-channel information leakage

Any idea?

• Using session keys
• Information hiding
• Information masking
Hiding

Goal: break the data-dependent power by using non-CMOS gates

- Dynamic differential logic: all I/O nodes turn to 1 in pre-charge stage, dual-rail I/O (always a pair of 0 and 1) in evaluation stage.
  - Sense-Amplifier-Based Logic (SABL)
  - Wave Dynamic Differential Logic (WDDL)
- Current-mode logic: use a constant current
  - MOS Current-Mode Logic (MCML)
- Asynchronous logic: timing information for DPA attack is obscured
Example: SABL NAND cell

(Courtesy to Mangard, Oswald and Popp’s paper)
Masking

Goal: introduce random power values into the total power traces

- Logic with randomness insertion: mask the data-dependent power by adding random bits into each logic gate.
  - Masked Dual-rail Pre-charged Logic (MDPL)
  - Random switching logic (RSL)
  - Dual-rail random switching logic (DRSL)
- Data scrambler
Example: MDPL NAND cell

(Courtesy to Mangard, Oswald and Popp’s paper)
System-level approaches

- Dynamic voltage and frequency switching approach
- Dummy logic: always adding and doubling operations to obscure the data dependence
- Duplication: separate the intermediate variable into two variables.
- High-level masking technique: the complier can analyze the encryption code and avoid the dependency of variables.
Weakness of countermeasures

- Unbalanced capacitive loads in hiding logic styles
- Memory effects and glitches
- Early propagation effects (some logic gates have reached new states before all gates have)
- ......

- DPA-specific countermeasures cannot defend other side-channel attacks
Conclusions

- Side-channel analysis attacks and countermeasures:
  - An ever-growing research area and a game
  - The advance of physical device and process technologies opens many opportunities
- Our research papers are available at http://www.rfid-cusp.org/publication.html
- UMass ECE and CS departments are active in embedded security research:

VLSI Circuits and Systems Group
University of Massachusetts Amherst

RFID
Consortium for Security and Privacy