Side-Channel Attacks

Xinmiao Zhang
Case Western Reserve University
Introduction

Side-channel attacks derive information about the secret key using specifics of the hardware implementation

- Passive attacks through observing physical data
  - Power analysis
  - Timing analysis
  - Electromagnetic analysis

- Active attacks by inserting faults through changing
  - Power supply voltage
  - Clock frequency
  - Temperature
  - Laser/radiation
Passive Attacks

- Physical and/or electrical effects unintentionally deliver information about the key
- Off-line analysis of the physical measurements allows to extract the key
  - **Simple attacks**: An attacker uses the side-channel information from one measurement directly to determine (parts of) the secret key.
  - **Differential attacks**: Many measurements are used to filter out noise. A hypothetical model is used to predict the side-channel information for pairs of plaintext and key. The predicted values are compared to the measured values to derive the key through correlation or pattern matching
Example for Simple Power Analysis

- Elliptic Curve Cryptography

1: \( Q \leftarrow P \)
2: \textbf{for} \( i \) \textbf{from} \( \ell - 2 \) \textbf{down to} \( 0 \) \textbf{do}
3: \( Q \leftarrow 2Q \)
4: \textbf{if} \( k_i = 1 \) \textbf{then}
5: \( Q \leftarrow Q + P \)
6: \textbf{end if}
7: \textbf{end for}

* S. Berna and O. Yalcin, "Side-channel attacks on hardware implementations of cryptographic algorithms"
Countermeasures for Simple Power Analysis

1: \( Q \leftarrow P \)
2: \( \text{for } i \text{ from } \ell - 2 \text{ downto } 0 \text{ do} \)
3: \( Q_1 \leftarrow 2Q \)
4: \( Q_2 \leftarrow Q_1 + P \)
5: \( \text{if } k_i = 0 \text{ then} \)
6: \( Q \leftarrow Q_1 \)
7: \( \text{else} \)
8: \( Q \leftarrow Q_2 \)
9: \( \text{end if} \)
10: \( \text{end for} \)

* S. Berna and O. Yalcin, "Side-channel attacks on hardware implementations of cryptographic algorithms"
Countermeasures for Passive Attacks

- Avoid branches conditioned by the secret bits
- Remove computation variations
- Time randomization
- Execution permutation
- Data masking
- Circuit-level modifications
Active Attacks: Effects of Faults in the AES

- Assumption: only one byte error happens during the last or the second to the last round of the AES en/decryption
- Information about the key can be derived by comparing the real cipher text and faulty cipher text

* N. Selmane and S. Guilley, "Practical setup time violation attacks on AES"
Inserting Faults Through Supply Voltage Reduction

- Lower voltage supply leads to longer propagation delay

* S. Bhasin, et. al. "Security evaluation of different AES implementations against practical setup violation attacks in FPGAs"
Probabilities of Generating Exploitable Faults

Composite field implementation

LUT-based implementation

* S. Bhasin, et. al. "Security evaluation of different AES implementations against practical setup violation attacks in FPGAs"
Open Problems

- Are there other implementations of the SubBytes more resistant to delay fault attack?
- How to make low-cost implementation of the AES algorithm more resistant to delay fault attack?
- Are there better countermeasures for other attacks?
- Are there efficient countermeasures against all or most types of attacks?