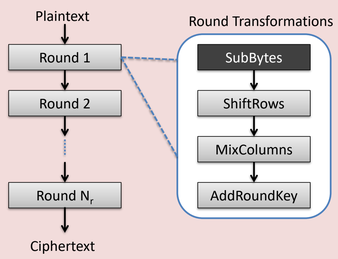
Investigating Power Analysis Attacks and Countermeasures for IoT Applications

Aaron Nguyen, Computer Engineering Program
Adviser: Dr. Jaya Dofe

Introduction

- Internet of Things (IoT) — refers to the billions of connected physical devices around the world, and changing the world we are living in
- Need for IoT technological security is at an all-time high and continues to grow.
- IoT can become secure through the proper use of cryptography for communication between the physical and cyber world
- However, emerging attacks side-channel analysis attacks are prominent in IoT
- Advanced Encryption Standard (AES) is used in industry and military encryption for secure communication
- Although AES is a secure algorithm, the hardware implementation of AES can leak data through the analysis of its hardware's physical properties (side-channel attack)

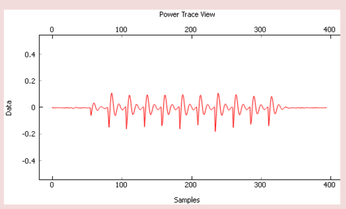
AES Design
https://cybersecurityglossary.com/aes/



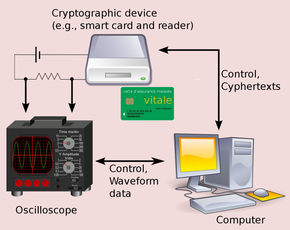
Encryption structure of AES algorithm

Power Side-Channel Attacks

- **Simple Power Analysis (SPA):** Visual inspections of a trace to gain more context. Useful if the attacker only has access to a few traces, but in general is difficult to use against AES
- **Differential Power Analysis (DPA):** Employs numerous statistical methods to derive the key. However, DPA requires many traces of the algorithm to work properly, often requiring many thousands of traces
- **Correlation Power Analysis (CPA):** Analyzes the data to find a correlation in power. Assumes the amount of power consumed is proportional to the number of bits with logic '1'



AES Power Trace

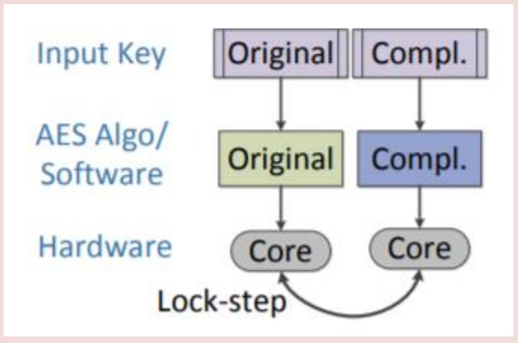


Power Analysis Setup
Power https://en.wikipedia.org/wiki/Power_analysis

Countermeasures for AES

Power Balancing

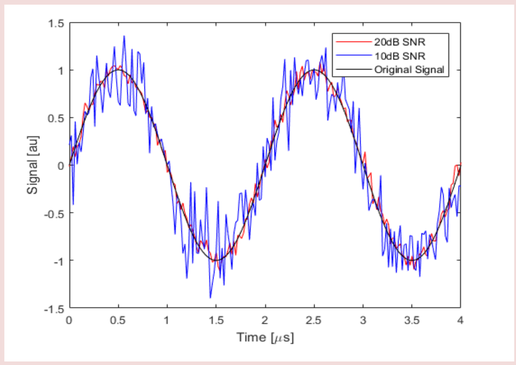
- Implementation technique where operations in the circuit consume an equal amount of power, causing power traces to become difficult to read



Algorithmic Balancing [1]

Noise Injection

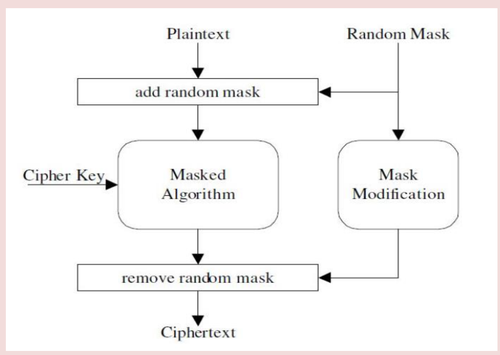
- Deliberately amplify or add noise in the circuit in order to make it difficult to analyze the power traces



Noise Injection Example

Masking

- Randomizes the intermediate values while keeping the input and output of a cipher the same as the unmasked. Technique can be applied to both hardware and software



Masking Design [2]

Countermeasures Against Power Attacks in IoT

False Key Based

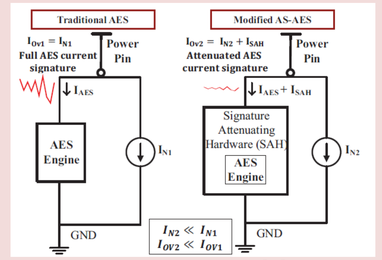
- Hardware design implementation that uses a fake encryption key to throw off CPA attacks [2]

Quantized Computing-Isolation Based

- Isolated hardware dedicated to prevent power analysis attacks on circuits [3]

Generic Countermeasure

- Hardware design implementation to dampens the amplitude of the power curve
- Allowing for the minimal noise injection necessary to resist power analysis attacks



AS-AES Design [4]

Summary

- Conventional cryptography is essential to secure the Internet and for IoT
- The design goals of IoT prioritize cost /energy efficient production, effectively leaving security implementation as an afterthought
- While there are no ways to absolutely prevent power analysis attacks, countermeasures can increase time/resources needed to determine the secret messages
- IoT designs need a security implementation that is strong enough to defend against power analysis attacks, yet minimalistic enough to maintain low power-consumption
- Properly implemented false key based, noise injection, and isolated security hardware designs are current methods to address power analysis security vulnerabilities
- Although power-analysis is the most common side-channel attack, it is not the only side-channel attack to be concerned about
- Analysis of a hardware's execution time, electromagnetism, and sound are other side-channel attacks that must be taken into consideration while designing the low-cost countermeasures
- For future work, we plan to design the secure AES system considering multiple side channels like fault, power, and electromagnetic

References

1. Arora et. al., "A Double-width Algorithmic Balancing to prevent Power Analysis Side Channel Attacks in AES"
2. *Weize Yu, Selçuk Köse. "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks"*
3. *Michael Moukarzel, Thomas Eisenbarth, Berk Sunar. "μLeech: A Side-Channel Evaluation Platform for IoT"*
4. Das et. al, "High Efficiency Power Side-Channel Attack Immunity using Noise Injection in Attenuated Signature Domain"