Side Channel Attacks and Neural Networks Notes

Michel Liao

June 2022

1 Introduction to Side-Channel Attacks

1.1 Introduction

- Based on this paper.
- **Side-channel cryptanalysis** considers adversaries trying to take advantage of the physical specificities of cryptographic devices.
- There are two ways to view a cryptographic primitive:[1]
  1. It's a "black box" that will output something when given an input.
  2. It's a program run on a processor, in an environment, and has specific characteristics.
- Physical attacks take advantage of specific characteristics to recover the parameters involved in the computation and are much more efficient than classical cryptanalysis.
- Physical attacks are often sorted on two orthogonal axes:
  1. **Invasive vs. non-invasive:** invasive requires getting direct access to a chip's components. Non-invasive exploits externally available information, e.g. running time, power consumption, etc.
  2. **Active vs. passive:** active tampers with the device's proper functions. Passive observes the device's behavior.
- Side-channel attacks are a class of physical attacks that exploit timing information, power consumption, or electromagnetic radiation. They are non-invasive and passive, making them usable by relatively cheap equipment.

[1] For now, think of it as a cryptographic algorithm. Look here for more information.

1.2 Basics of Side-channel Attacks

1.2.1 Origin of the Leakages

Power consumption.

- We focus on CMOS gates[2] because they're widely used.
- Static CMOS gates have 3 distinct dissipation sources:
  1. Leakage currents in transistors,
  2. the switching of a gate while NMOS and PMOS are conducting simultaneously,
  3. and the dynamic power consumption due to the charge and discharge of load capacitance.
- Dynamic power consumption is externally observable, giving us information about internal data.

EM Radiation in CMOS Devices

- Electromagnetic leakages are explained by the Bio-Savart law:

$$d\vec{B} = \frac{\mu I \, d\vec{l} \times \hat{r}}{4\pi r^2}.$$

  - The field is data-dependent because of the dependence on current intensity
  - and the field orientation depends on the current direction.

Leakage Models

- The **Hamming distance model** and **Hamming weigh model** correlate information about side-channel leakages with distance and weights.
- Other models improve on these models by using advanced statistical tools.

1.2.2 Measurement Steps

-

1.3 Classical Attacks: SPA and DPA

- **Simple Power Analysis (SPA)** interprets the power consumption of a device and deduces information about its performed *operations*.
- **Differential Power Analysis (DPA)** tries to take advantage of *data* dependencies in power consumption patterns.

[2] These are essentially switches that aren't restricted to having either $0\,A$ current or a constant, non-zero current. They can have a current within a range from 0 to a non-zero value.

2 Correlation Power Analysis with a Leakage Model

- Based on this paper.