Power Analysis Setup

Nicolas Potvin

Contents

Introduction

Power analysis attacks are all types of side channel attacks based on power comsumption of a piece of hardware dedicated to data encryption. The aim of these attacks is to discover the secret stored in the device. It is important to note that these attacks target the hardware on which is implemented the encryption algorithm, not the algorithm itself. This means that these attacks are based only on the knowledge of the plain data and the power that is being used to encrypt the data, not on the exploitation of a faulty bahvior of the algorithm or to make it reveal its secret by any other means based on data manipulation.

To achieve such an attack the attacker must have a physical access to the device. It is best to know the details of the internal circuits of the device to estimate its power consumption. But attackers have almost never access to that information. Therefore a model must be established to approximate the circuit based on clues about its design and general knowledge about encrypting devices. The model must fit the reality to permit a successful attack, if it does not approximate well enough the actual circuit it can lead to false results appearing to be the expected ones to the attacker.

These attacks are the center of great interest because of their effectiveness and their low equipment requirement. Which is very good for an attacker, but far less for those concerned about security. this concern naturally leads to the search of effective countermeasures and masking. This article will mainly focus on the attacks and more specificaly on the setup necessary to conduct these attacks.

Components

General Setup

Conducting an attack