Power analysis attacks

Sergei Skorobogatov

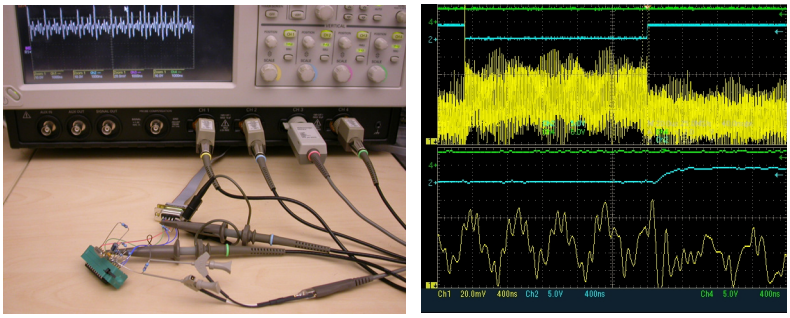
UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Introduction to power analysis

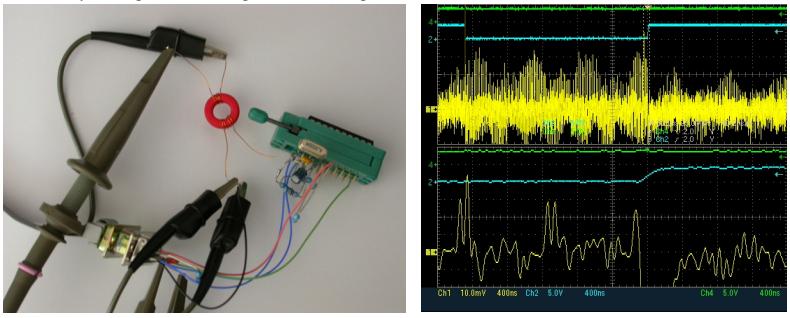
Most digital circuits are based today on CMOS technology, using complementary transistors as a basic element. When a CMOS gate changes its state, it charges/discharges a parasitic capacitive load and causes a dynamic short circuit of the gate. The more gates changing their state, the more power is dissipated. The current consumed by a circuit can be measured by placing a small resistor or a transformer in the power supply line.

Drivers on the address and data bus consist of many parallel inverters per bit, each driving a large capacitive load. During transition they cause a significant power surge in the order of 0.5–1 mA per bit, which is sufficient to estimate the number of bus bits changing at a time. By averaging the measurements of many repeated identical operations, smaller transitions can be identified. Of particular interest for cryptographic algorithms is the state change of a carry bit.

In order to reconstruct the algorithm or find the secret key, power consumption measurements for different input data are normally done with a digitizing oscilloscope at a few hundred megahertz. After that, the acquired traces are transmitted to a computer for comparison and post processing.

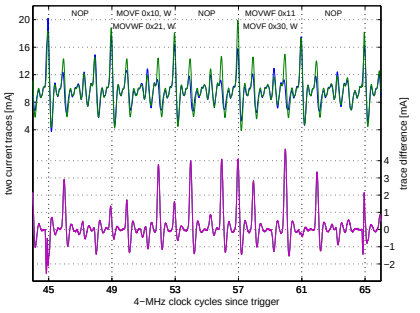


Power analysis setup and oscilloscope waveforms acquired from MC68HC908JB8 microcontroller

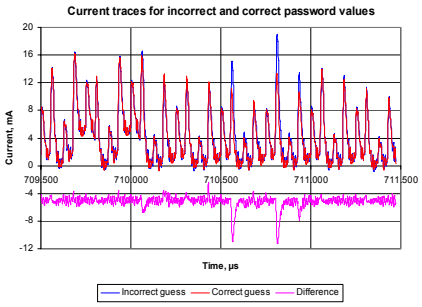


Power analysis using a transformer and oscilloscope waveforms acquired from the same microcontroller

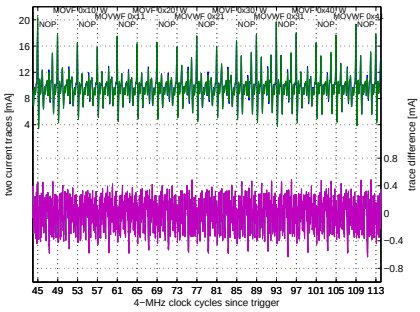
Instruction, address and data dependency



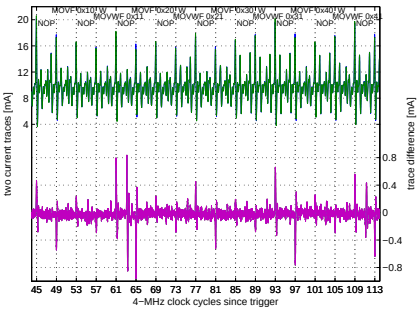
Difference between instructions in a PIC16F84 microcontroller



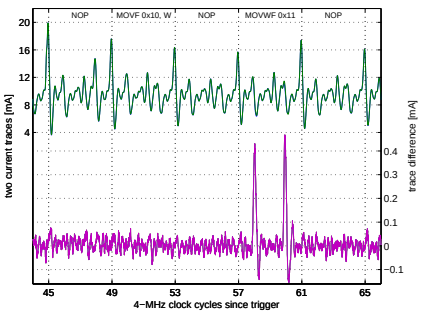
Guessing the password in a HC908AZ60A microcontroller



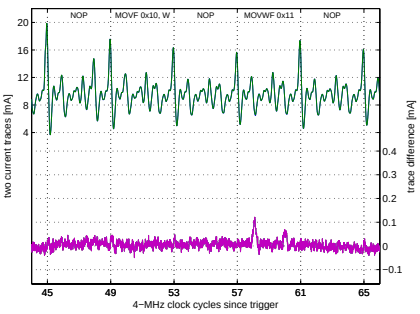
Difference between traces from two samples of PIC16F84



Difference between the same code run at different addresses



Difference between (0x00 → 0x00) and (0x01 → 0x00), Av=64



Difference between (0x01 → 0x00) and (0x10 → 0x00), Av=256

Each type of instruction executed by a CPU causes different levels of activity in the instruction decoder and arithmetic unit, therefore it can often be clearly distinguished, making it possible to reconstruct passwords and parts of algorithms.

Power traces acquired from two identical samples may be different because of fabrication variations between devices – different location on the wafer, slight size variations in transistors and wires, variations in leakage currents and parasitic capacitance. This results in a large residual difference when two traces from different samples are compared. Therefore, power traces from the same device are more easily compared.

Even for the same portion of code running on the same device the power traces can be different if the code is executed from different memory locations, because address decoders also contribute to the power consumption.

When looking for data, for example in a cryptographic operation, it is important to understand that the power fluctuations are affected by the number of bits set or reset. As a result, only the Hamming weight of data (number of bits set) can be estimated, rather than the actual value. However, because of small variations between transistors on the chip and different lengths of wires, there is still a small difference in power traces, even for the same Hamming weights. For some Hamming weights, such as one or the bus width minus one, it is practical to distinguish between data values by averaging a large number of traces, thus reducing the noise and increasing the resolution.