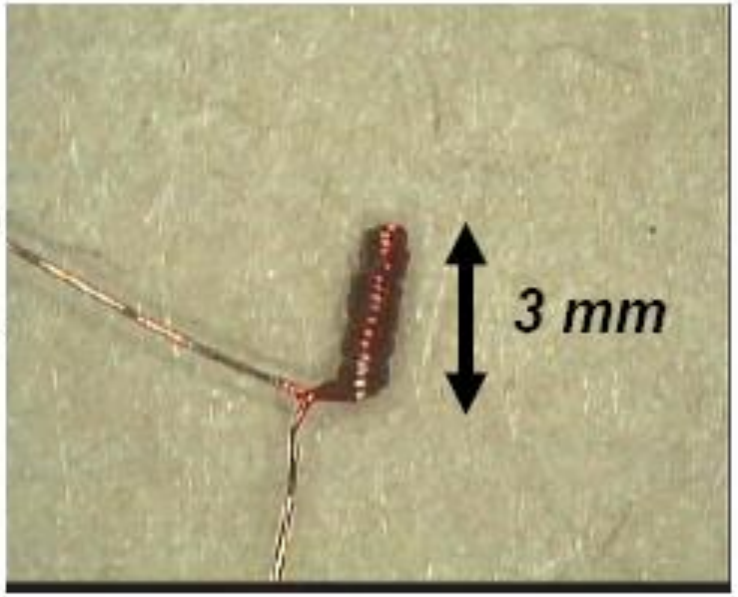
Electromagnetic Power Analysis

EM radiation is correlated to the switching activities of CMOS gate circuits. Inductive probes are used to capture the EM radiation caused by switching activities of CMOS gate circuits inside the chips. The probe itself should be small enough to enable accurate location.

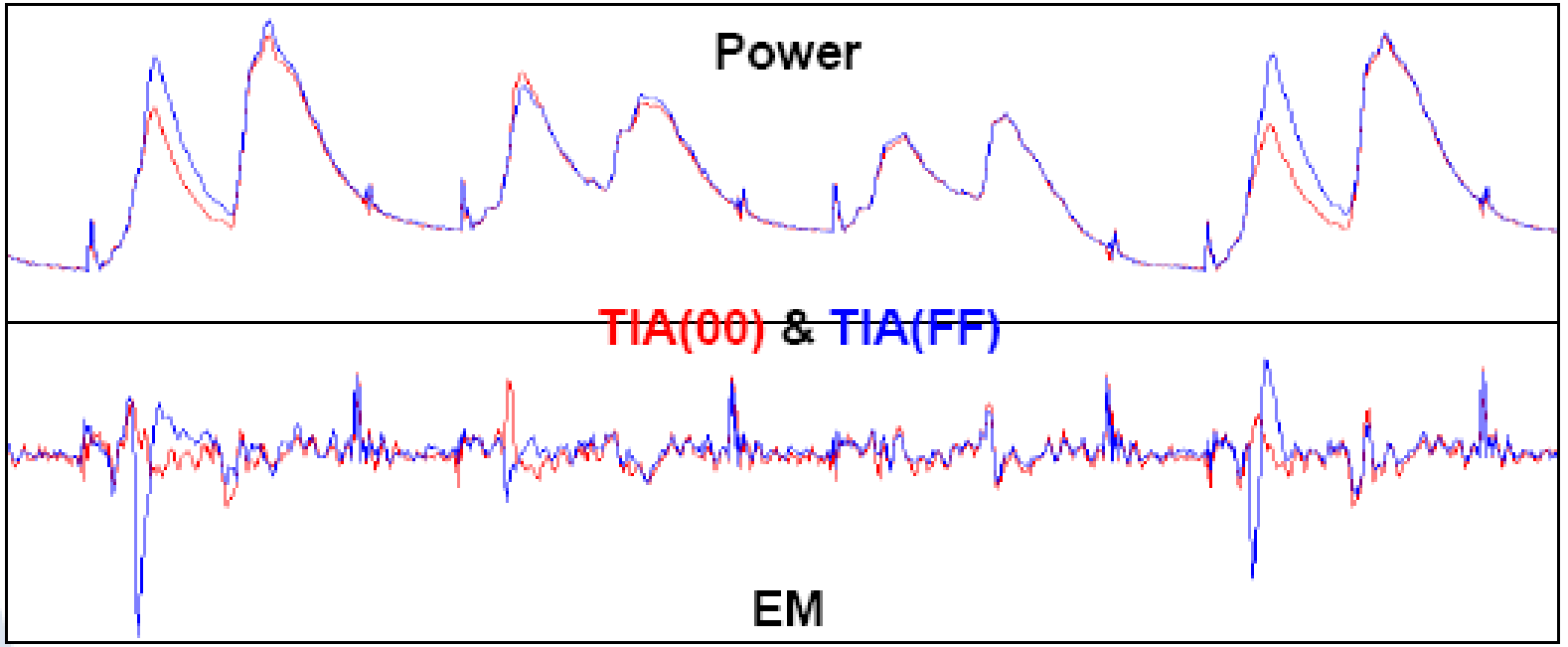
EMA – probe design

- Hamming distance model for information leakage
  Correlated to the number of flipping bits (CMOS, VLSI)
- Electrical transitions disturb EM near field (and its flow ϕ)
- Captation by inductive probe
  - Handmade solenoid $V = -\frac{d\phi}{dt}$
    (Diameter = 150 to 500 µm)
  - Difficult to calibrate
    (Bandwidth > 100 MHz, low voltage, parasitic effects)
  - Good acquisition chain required, but no Faraday cage
    (Sampling at 1GHz)



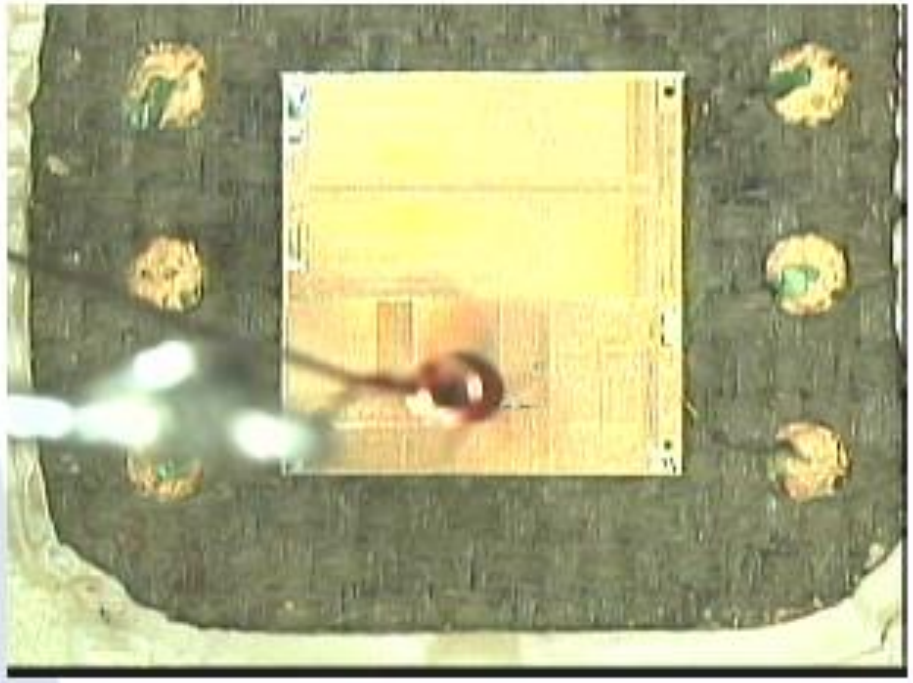
EMA signal

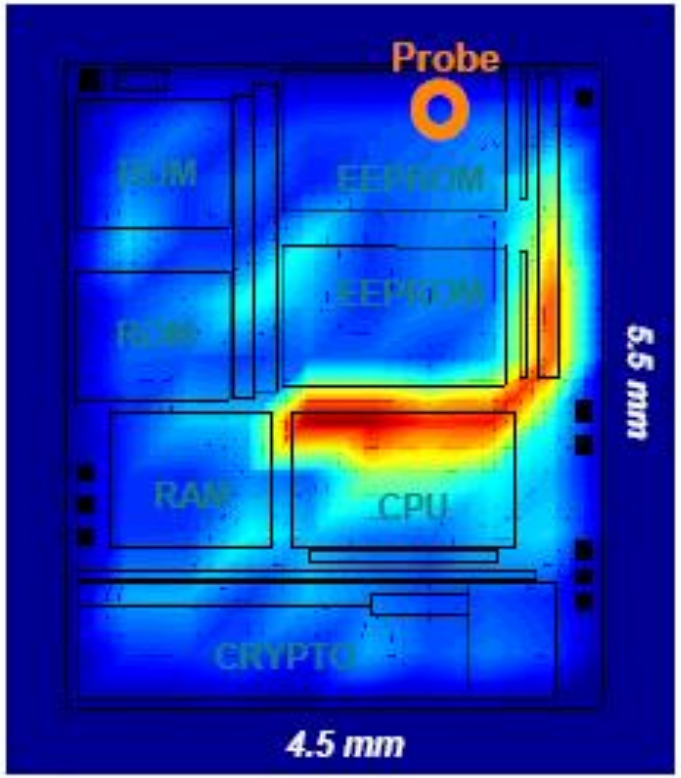
- Raw signals (TIA : transfer into accumulator instruction)
  - Power is less noisy
  - But EM signatures are sharper !



Spatial Positioning

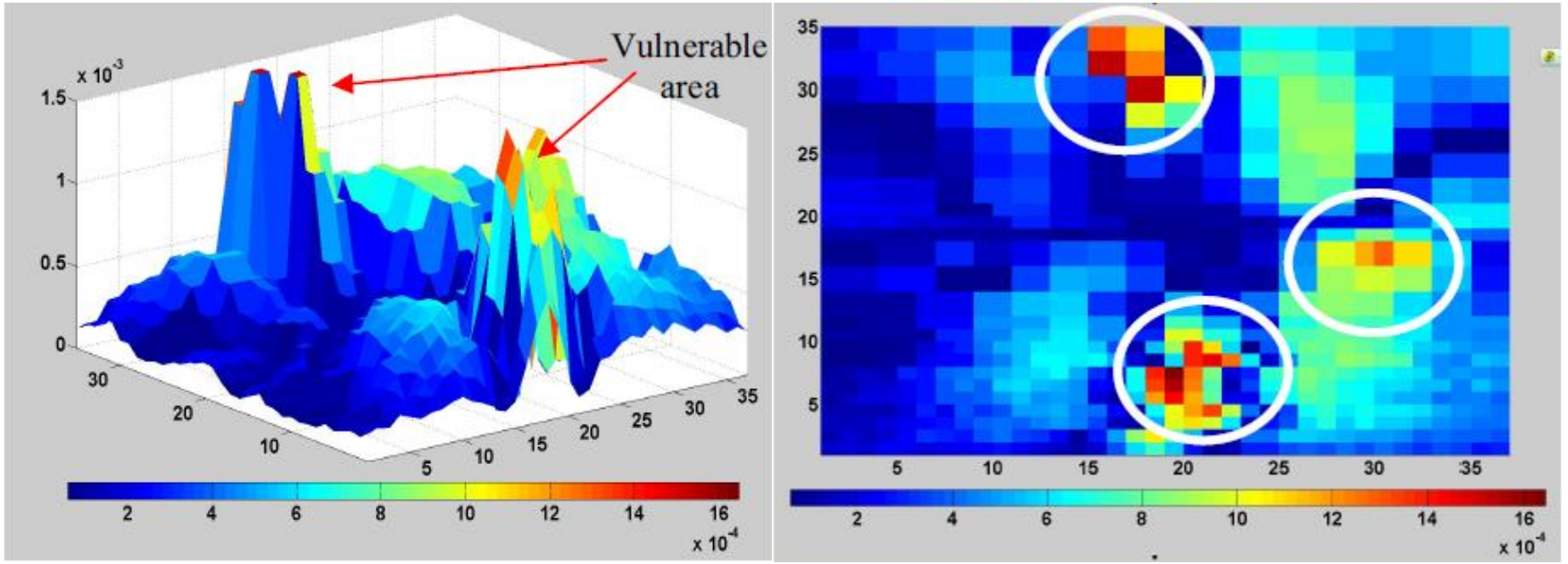
- Horizontal cartography (XY plane)
  - to pinpoint instruction related areas
  - better if automated





Inductive probes can be used to pinpoint instruction related areas.

Spectral density of the chip surface



Spectral density distribution of the chip surface, which is correlated to the functional modules distribution, are shown in this figure.

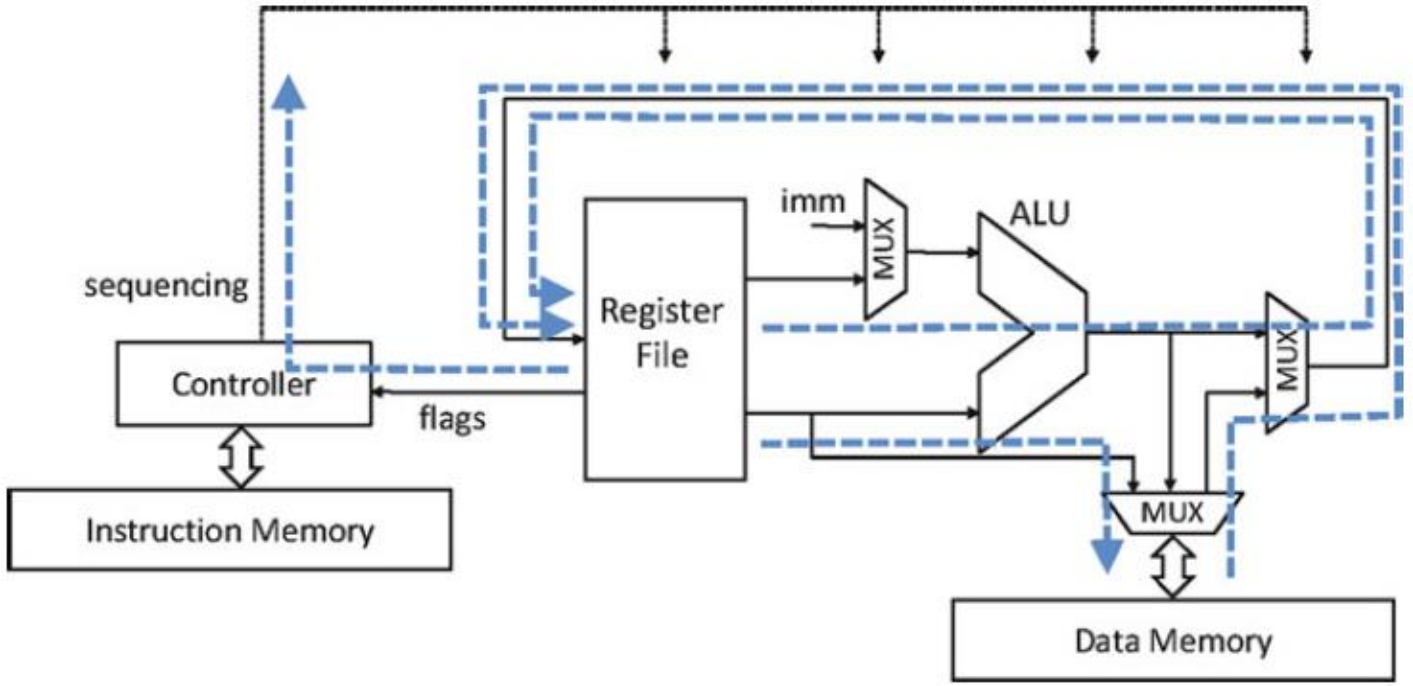
EMA

- Advantage of EMA versus PA
  - Local information more “data correlated”
  - EMA bypasses current smoothers
  - EMA goes through HW countermeasures: shields, randomized logic
- Drawbacks
  - Experimentally more complicated
  - Geometrical scanning can be tedious
  - Low level and noisy signals (decapsulation required)

Countermeasures

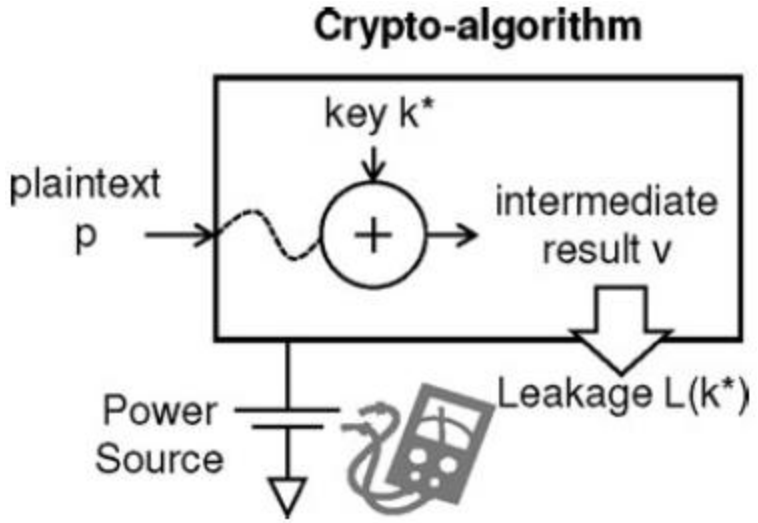
- Software (crypto routines)
  - Coding techniques
  - Same as anti DPA/SPA (data whitening…)
- Hardware (chip designers)
  - Confine the radiation (metal layer)
  - Blur the radiation (e.g. by an active emitting grid)
  - Reduce the radiation (technology trends to shrinking)
  - Cancel the radiation (dual logic)

Source of side-channel leakage in a microcontroller



- Memory-store instructions
- Memory-load instructions
- Arithmetic instructions
- Control-flow instructions

Side-Channel Attacks on Microcontrollers



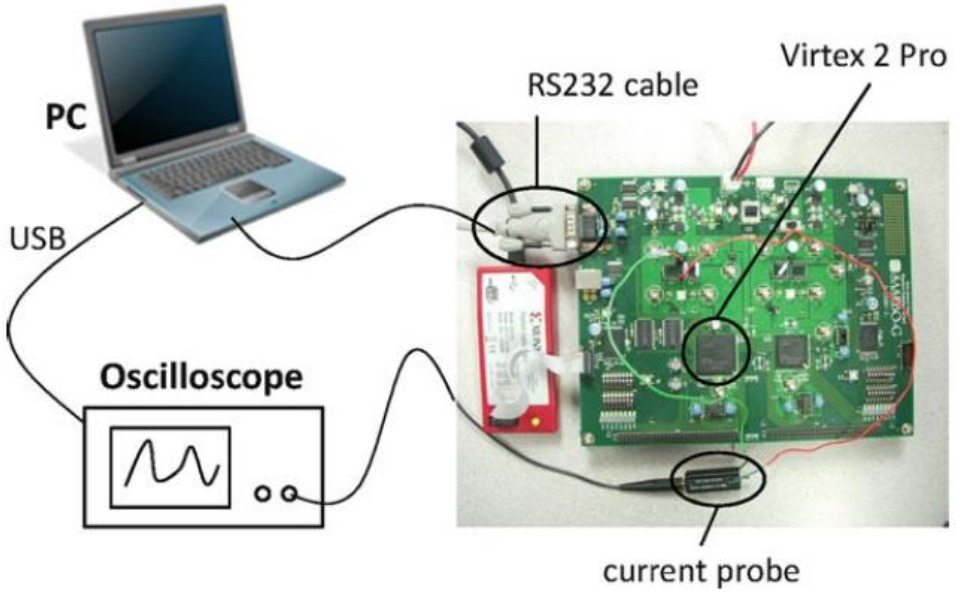
Objective: retrieve the internal secret key k^* of a crypto-algorithm

- The leakage caused by v is a function of the key value k^*, and it can be expressed as follows:

$$L(k^*) = f_{k^*}(p) + \varepsilon$$

The function f_{k^*} is dependent on the crypto-algorithm as well as on the nature of the implementation in hardware and software. The error ε is an independent noise variable.

Side-Channel Attacks on Microcontrollers



- The PC sends a sample plaintext to the PowerPC on the FPGA for encryption. During the encryption, the digital oscilloscope captures the power consumption from the board. After the encryption is completed, the PC downloads the resulting power trace from the oscilloscope, and proceeds with the next sample plaintext.

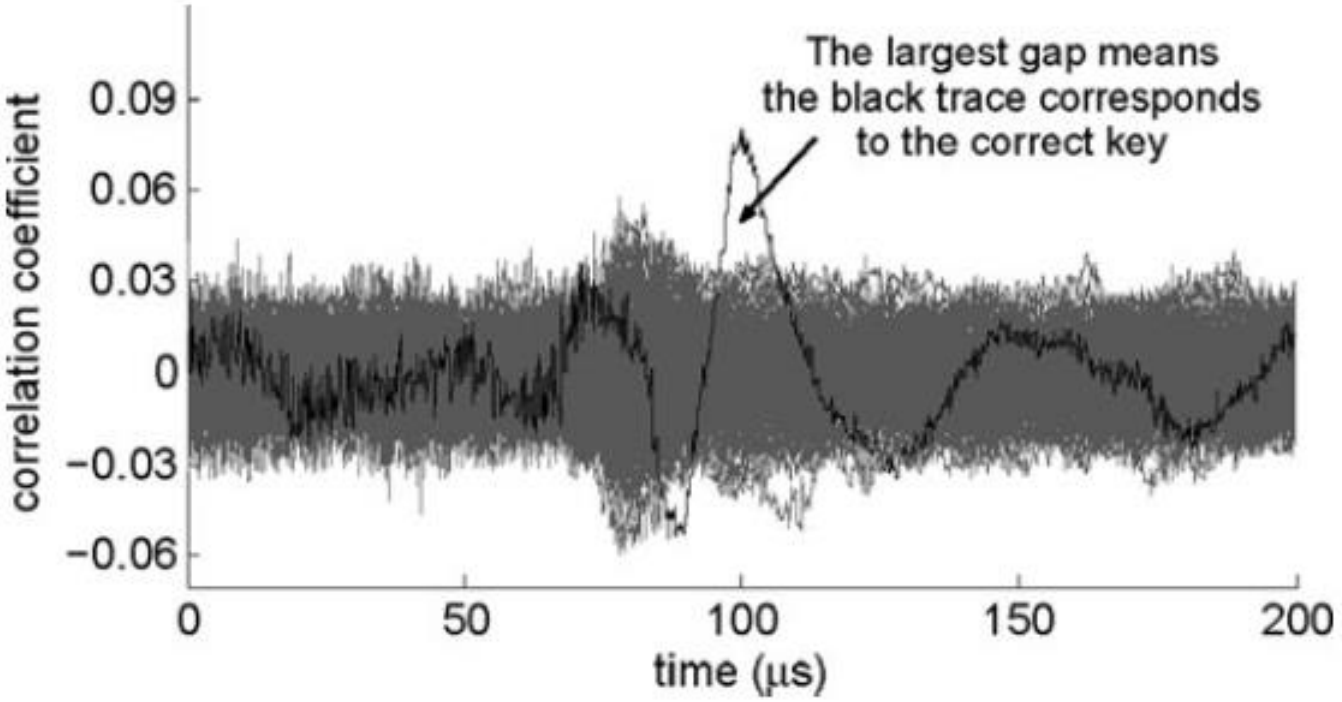
CPA: Correlation Power Analysis

- Two important aspects of a practical CPA:
  - The selection of the power model

    The power model is chosen so that it has a dependency on a part of the secret key. A good candidate is the output of the substitution step.
  - The definition of the attack success metric

    Measurements to Disclosure (MTD): the more measurements that are required to successfully attack a cryptographic design with side-channel analysis, the more secure that design is.

Practical Hypothesis Tests



- An example of 256 correlation coefficient traces. Around time 100 us, the black trace which corresponds to the correct key byte emerges from all the other 255 traces.

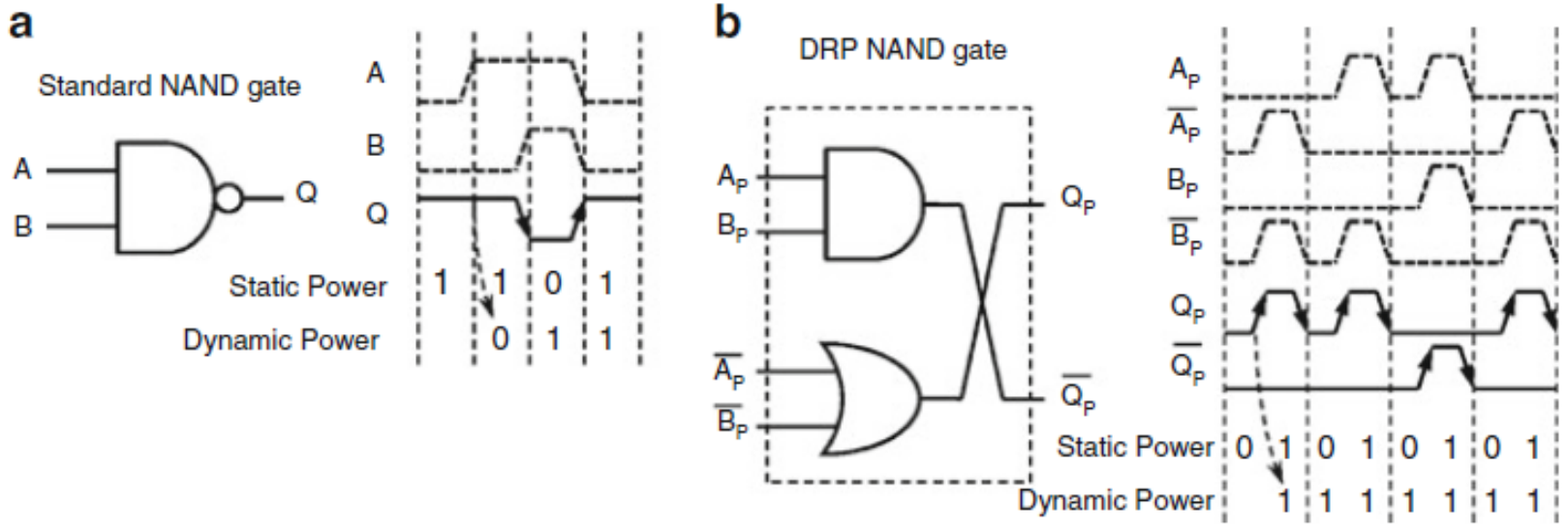
Side Channel Countermeasures for Microcontrollers

- Two different kinds of countermeasures:
  - Algorithm-Level Countermeasures

    Transform the C program so that the generation of dangerous side-channel leakage is avoided.
  - Architecture-Level Countermeasures

    Create a better microcontroller, for example using special circuit techniques, so that no side-channel leakage is generated.

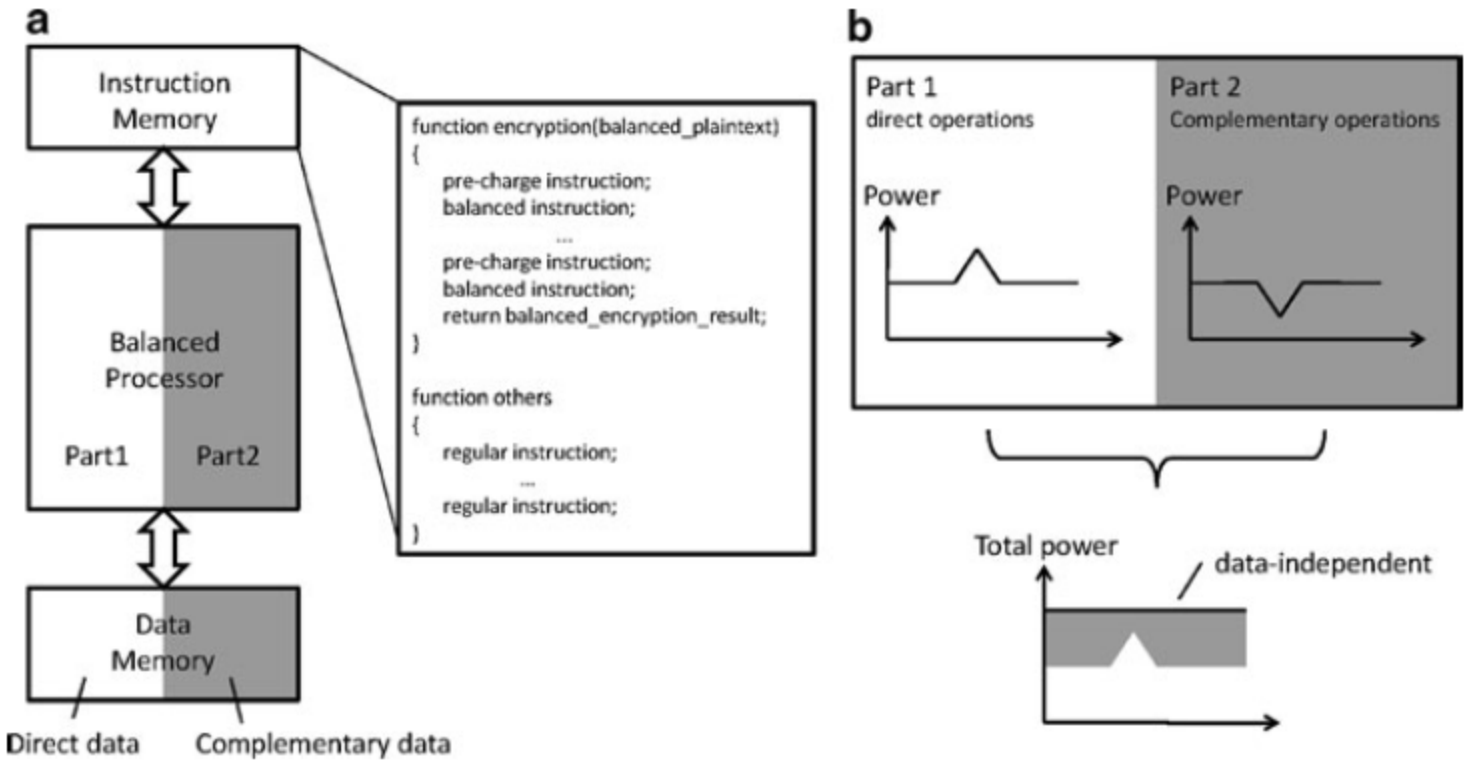
Dual Rail Precharge



- (a) A CMOS standard NAND has **data-dependent** power dissipation;
- (b) A DRP NAND gate has a **data-independent** power dissipation

- DRP requires the execution of the direct and complementary data paths in parallel.

Virtual Secure Coding: Porting DRP into software



- (a) Concept of balanced processor and VSC programming;

  (b) The balanced processor does not show side-channel leakage

- The power dissipation from the direct operation always has a complementary counterpart from the complementary operation. The sum of these two is a constant.