SIDE-CHANNEL ATTACKS ON IMPLEMENTATIONS OF CRYPTOGRAPHIC ALGORITHMS

Assoc. Prof. Dr. Sıddıka Berna Örs Yalçın

Istanbul Technical University

Department of Electronics and Communication Engineering

Motivation

- For implementations of cryptographic algorithms, not only the speed and the size of the circuit, but also their security against implementation attacks such as side-channel attacks are important.
- Side-channel attacks are mentioned in Common Methodology for Information Technology Security Evaluation.

Introduction

- A side-channel analysis attack takes advantage of implementation specific characteristics
- Divided into two groups as
  - active (tamper attacks): the attacker has to reach the internal circuitry} of the cryptographic device
    - probing attack: inserting sensors into the device
    - fault induction attack: disturbing the device's behavior
  - passive: The physical and/or electrical effects of the functionality of the device are used for the attack

Passive Attacks

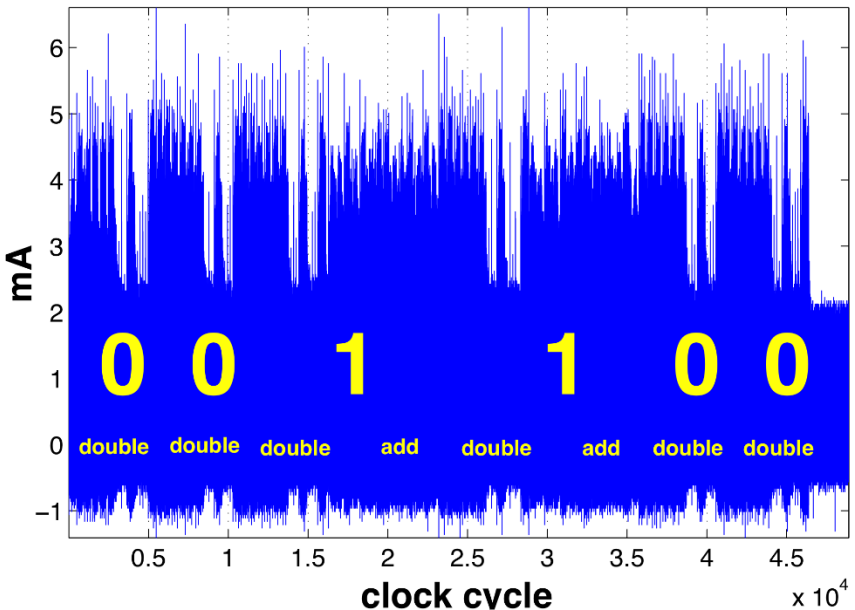
If physical and/or electrical effects unintentionally deliver information about the key, then they deliver side-channel information and are called side-channels.

Four groups according to the side-channel information that they exploit:

- Timing Analysis Attack
- Power Analysis Attack
  - Simple Power Analysis (SPA)
  - Differential Power Analysis (DPA)
- Electromagnetic Analysis attacks
  - Simple Electromagnetic Analysis (SEMA)
  - Differential Electromagnetic Analysis (DEMA)
- Fault based attacks

Simple Attacks

- An attacker uses the side-channel information from one measurement directly to determine (parts of) the secret key.
- A simple analysis attack exploits the relationship between the executed operations and the side-channel information.

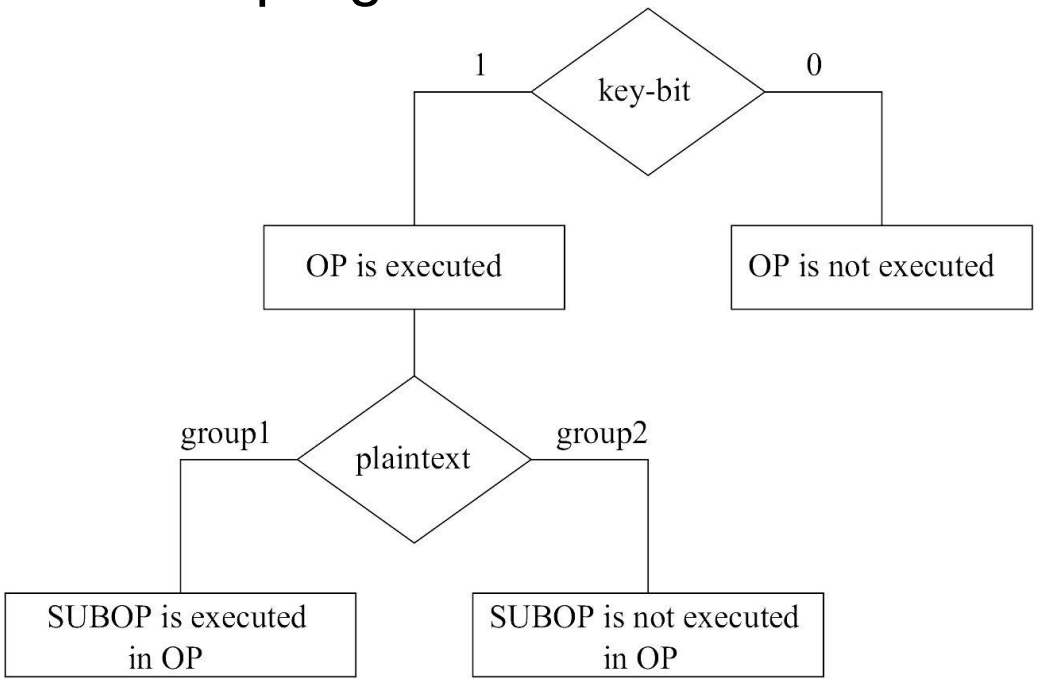


Differential Attacks

- Many measurements are used in order to filter out noise.
- A differential analysis attack exploits the relationship between the processed data and the side-channel information.
  - hypothetical model of the attacked device: The model is used to predict several values for the side-channel information of a device.
  - These predictions are compared to the real, measured side-channel information of the device.
  - Comparisons are performed by applying statistical methods on the data.

Timing Analysis Attack

- The differences in the processing time of a hardware or software system may vary with the code sequence and processed data sets. Checking time may in unsecured systems retrieve secret information.
  - If the test of specific values and a following dependent branch in the program code is not secured.



Timing Analysis Attack (Cont.)

the Hamming weight of the key: when the execution time depends on the secret key $\rightarrow$ only one measurement needed

EC point Multiplication

$Q \leftarrow P$

for i from l-2 downto 0

$Q \leftarrow 2Q$

if k_i=1

$Q \leftarrow Q+P$

Execution time of one point multiplication:

$T_{PMUL}=(l-1)T_{PDB}+(w-1)T_{PAD}$ (w= Hamming weight of the key)

Countermeasure for Simple Timing Attack

- Input: EC point $P=(x,y)$, integer k, $0 < k < M$, $k=(k_1, k_2, \ldots, k_{l-1})_2$, $k_{l-1}=1$ and M
- Output: $Q=[k]P=(x',y')$
  - $Q = P$
  - for i from $l-2$ downto 0
    - $Q_1 = 2Q$
    - $Q_2 = Q_1 + P$
    - If $k_i=0$
      - $Q = Q_1$
    - else
      - $Q = Q_2$
- The latency of one point multiplication:
- $T_{PMUL}=(l-1)\ (T_{PDB}+T_{PAD})$

Differential Timing Attack on a Hardware Implementation of AES (1/2)

- The input of the first S-Box operation in the first round is the first byte of the output of the
- AddRoundKey(Plaintext,Key)=Plaintext xor Key.
- S-Box Operation in AES
- Input: one byte *in*
- Output: *out*=S-Box(*in*)
- *Step1: out*=AffTrans(*in*)
- *Step2:* If *out*=0
  - *Step3: out=0*
- *Else*
  - *Step4: out=MultInv(out)*

DTA on a Hardware Implementation of AES (2/2)

- Step 3 is executed in shorter time than Step 4. The attacker's steps:
  1. Feed the hardware with *N* plaintexts
  2. Measure the time which takes for encrypting each of them and form a $N \times 1$ matrix M_1 with these timing data.
  3. Calculate Plaintext xor Key for *N* plaintexts for each possible 256 values of the first byte of the key and for each plaintext.
  4. Form a $N \times 256$ matrix M_2 with the expected time of S-box (AffTrans(Plaintext xor Key) operation.
  5. Now the attacker should find the correlation between M_1 and each column of M_2. The highest correlation will give the right first byte of the key.

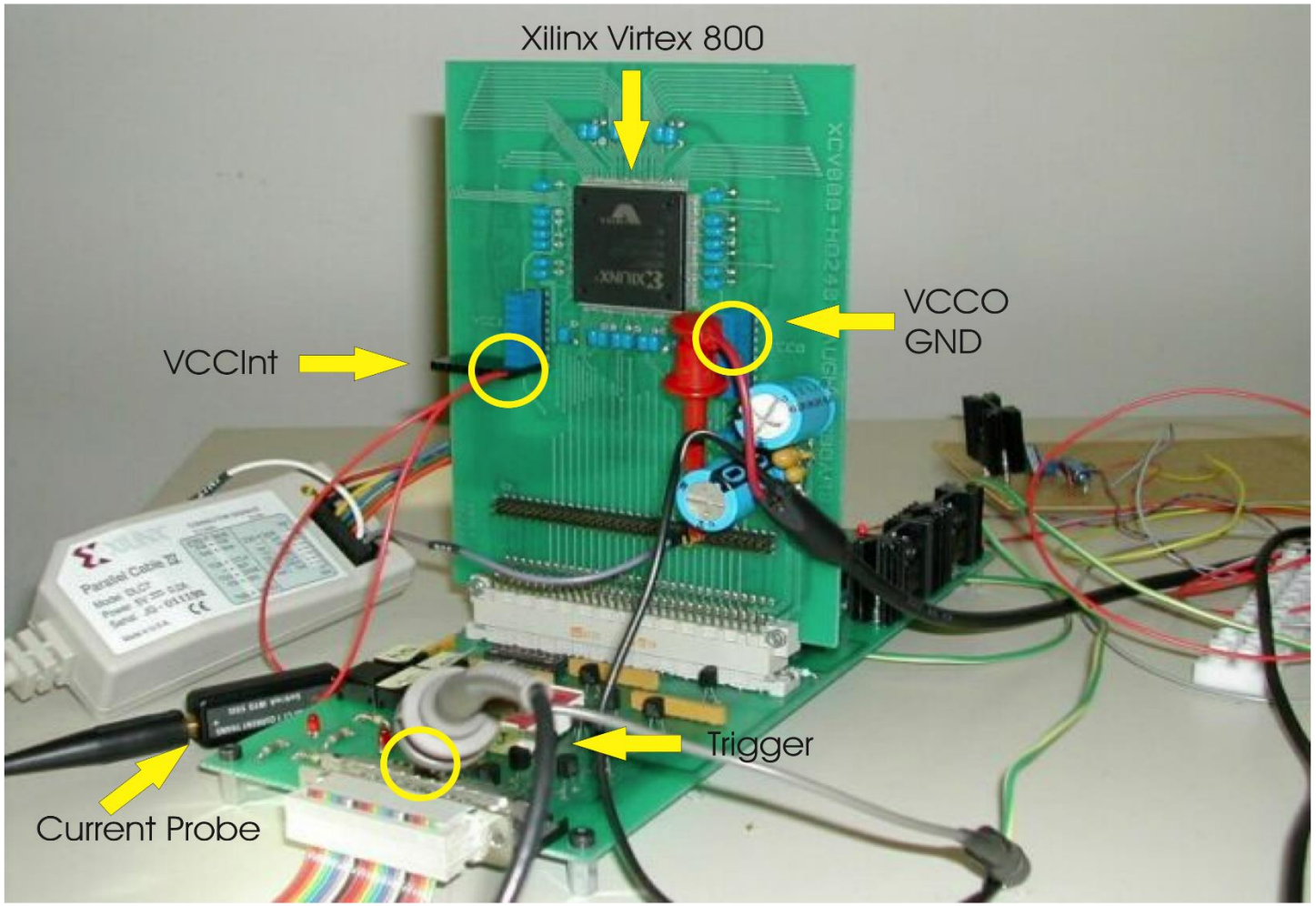
Power Attacks

- The dominating factor for the power consumption of a CMOS gate is the dynamic power consumption:
- $P_D = C_L V_{DD}^2 P_{0\rightarrow 1} f$

Power Attacks

- We will observe a current only during the 0 → 1 transition at the output of the circuit.
- This transition depends on the input of the circuit, so the processed data in the gate.
- By observing the current consumption of a circuit we can learn some information about the processed data.
- If this data has some relation with the secret information than we gain some information about the secret.

Measurement Setup



Simple Power Analysis Attack (SPA)

EC point Multiplication

$Q \leftarrow P$

for i from l-2 downto 0

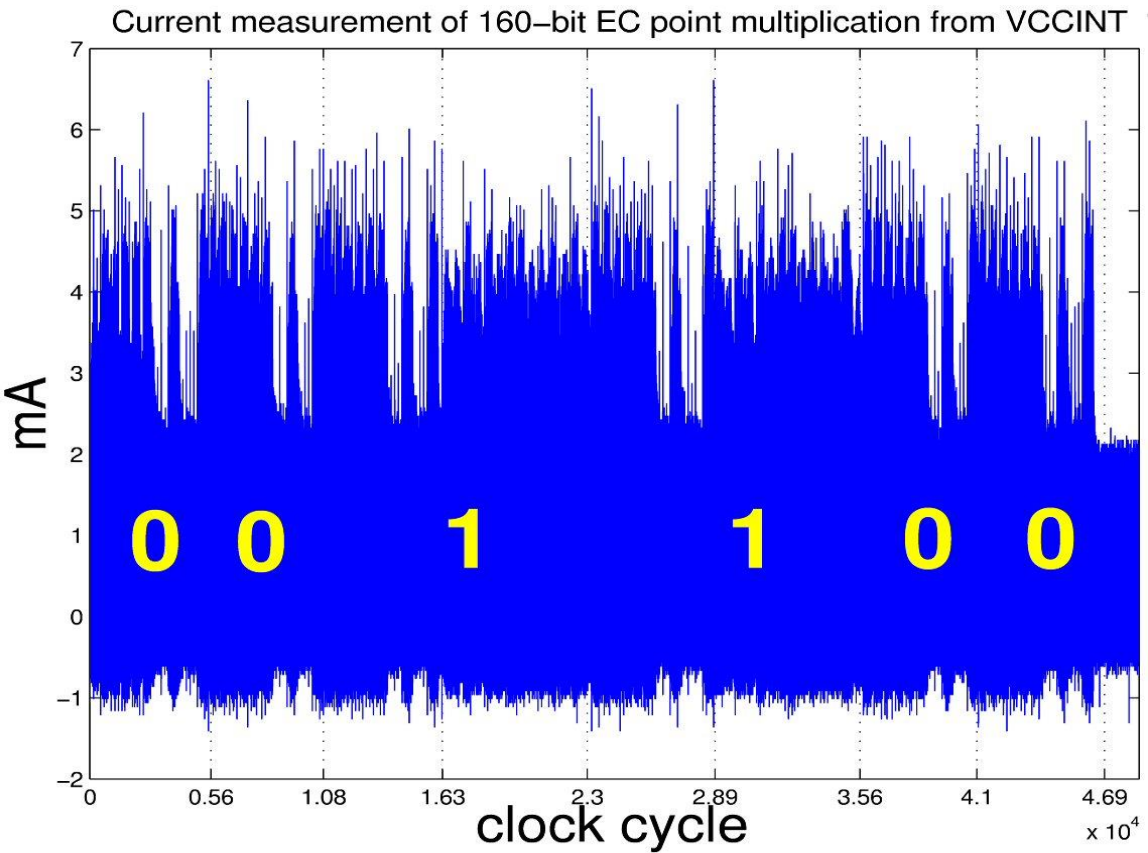
$Q \leftarrow 2Q$

if k_i=1

$Q \leftarrow Q+P$

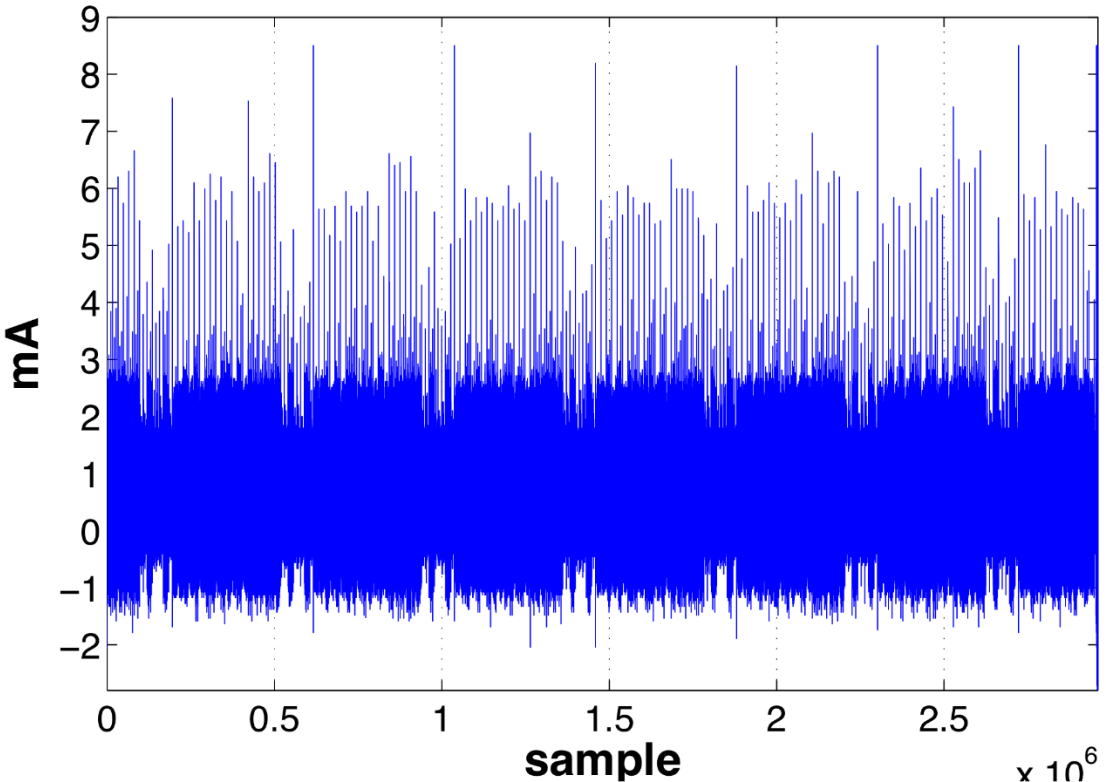
- point double and add

consume different power



Countermeasure for SPA on an Implementation of ECC

- Input: EC point $P=(x,y)$, integer k, $0 < k < M$, $k=(k_1, k_2, \ldots, k_{l-1})_2$, $k_{l-1}=1$ and M
- Output: $Q=[k]P=(x',y')$
  - $Q = P$
  - for i from $l-2$ downto 0
    - $Q_1 = 2Q$
    - $Q_2 = Q_1 + P$
    - If $k_i=0$
      - $Q = Q_1$
    - else
      - $Q = Q_2$

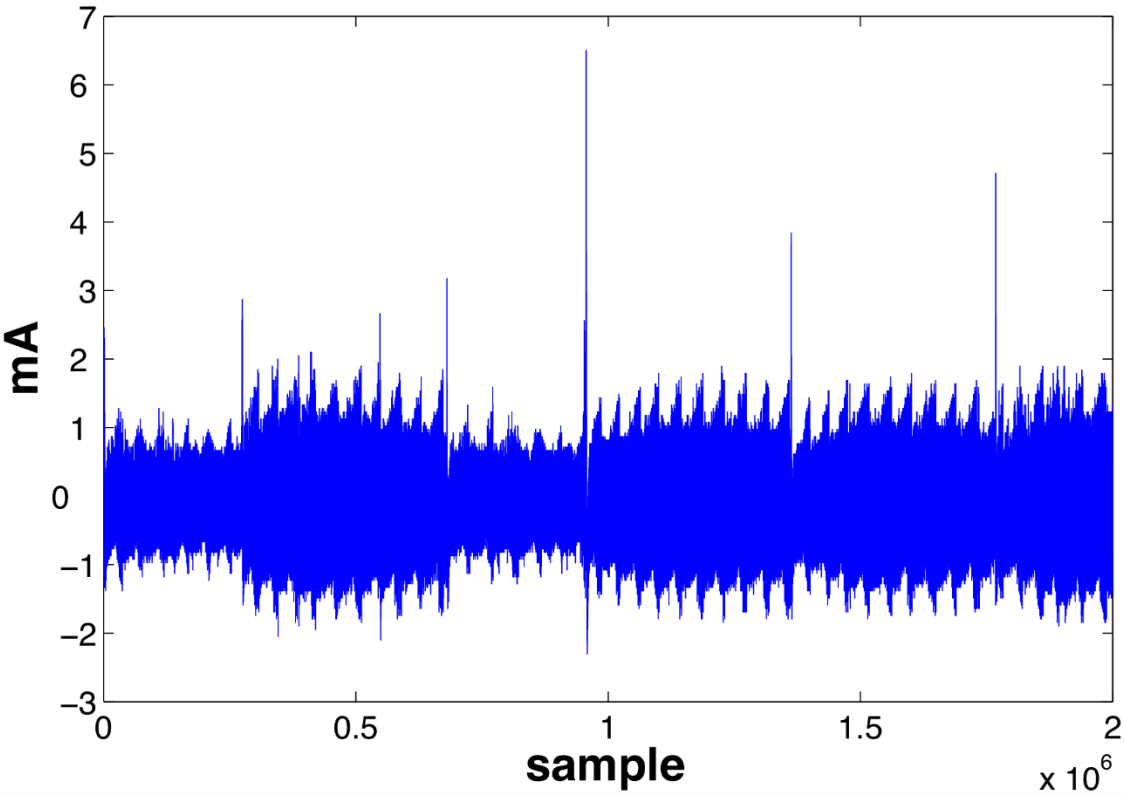


Differential Power Analysis of an Implementation of ECC

- The target is k_{l-2}.
- The points Q_1, Q_2 and Q are updated as:
  - $Q = P$
  - $Q_1 = 2Q = 2P$
  - $Q_2 = Q_1 + P = 3P$
  - If k_{l-2}=0
    - Q changes from P to 2P
  - else
    - Q changes from P to 3P

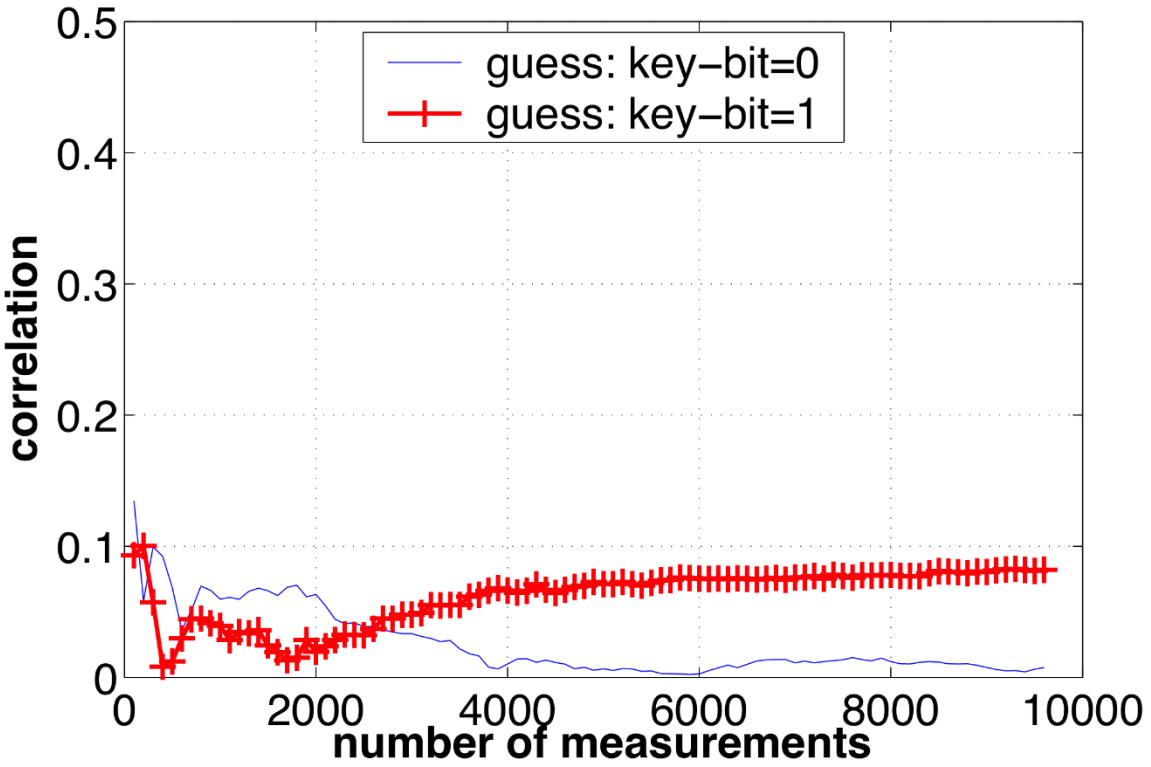
Correlation Analysis (1/2)

- Chosen *N* random points on the EC
- FPGA executes *N* point multiplications such that $Q_i=[k]P_i$
- measured the power consumption
- produced a matrix, M_1

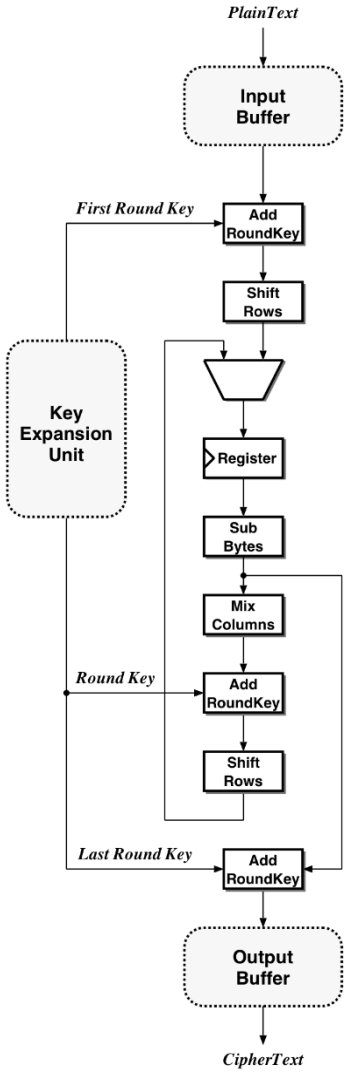


Correlation Analysis (2/2)

- Compute *N* EC point multiplications
- Compute the number of bit transitions from 0 to 1 in Q
  - for $k_{l-2} = 0$: the number of transitions between P to 2P, (M_2)
  - for $k_{l-2} = 1$: the number of transitions between P to 3P, (M_3)
- If the correlation between M_1 and M_2 is higher than the correlation between M_1 and M_3, $k_{l-2} = 0$, otherwise $k_{l-2} = 1$



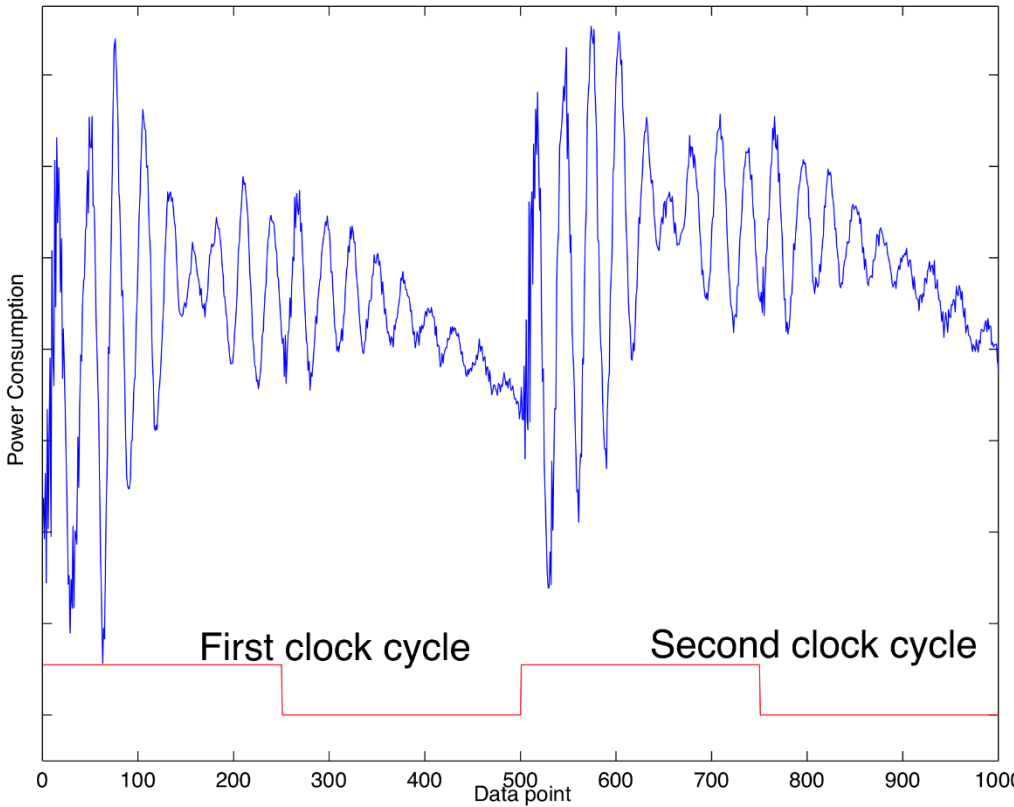
DPA on an ASIC Implementation of the AES



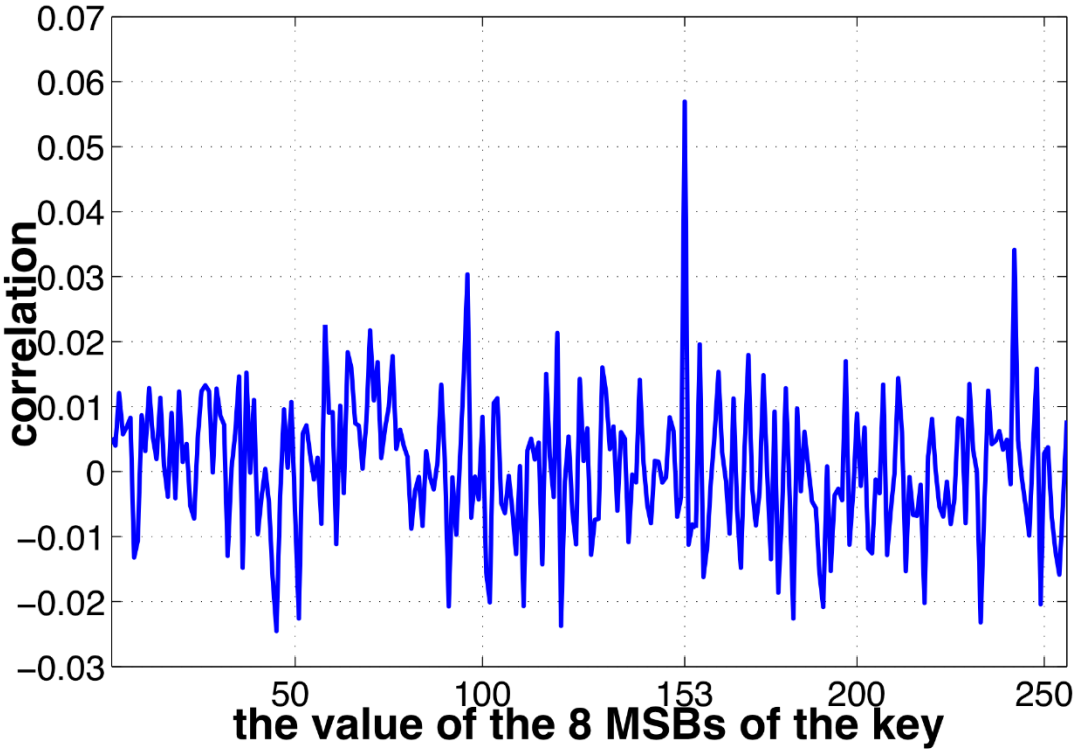
- Fastcore was designed by ETH Zurich
- The target for our DPA attack are the most significant byte of the Register

Power Consumption of 1 Encryption with Fastcore

- Encrypt *N* plaintexts with a random but fixed key.
- Measure the current consumption
- Calculate the mean value of the data

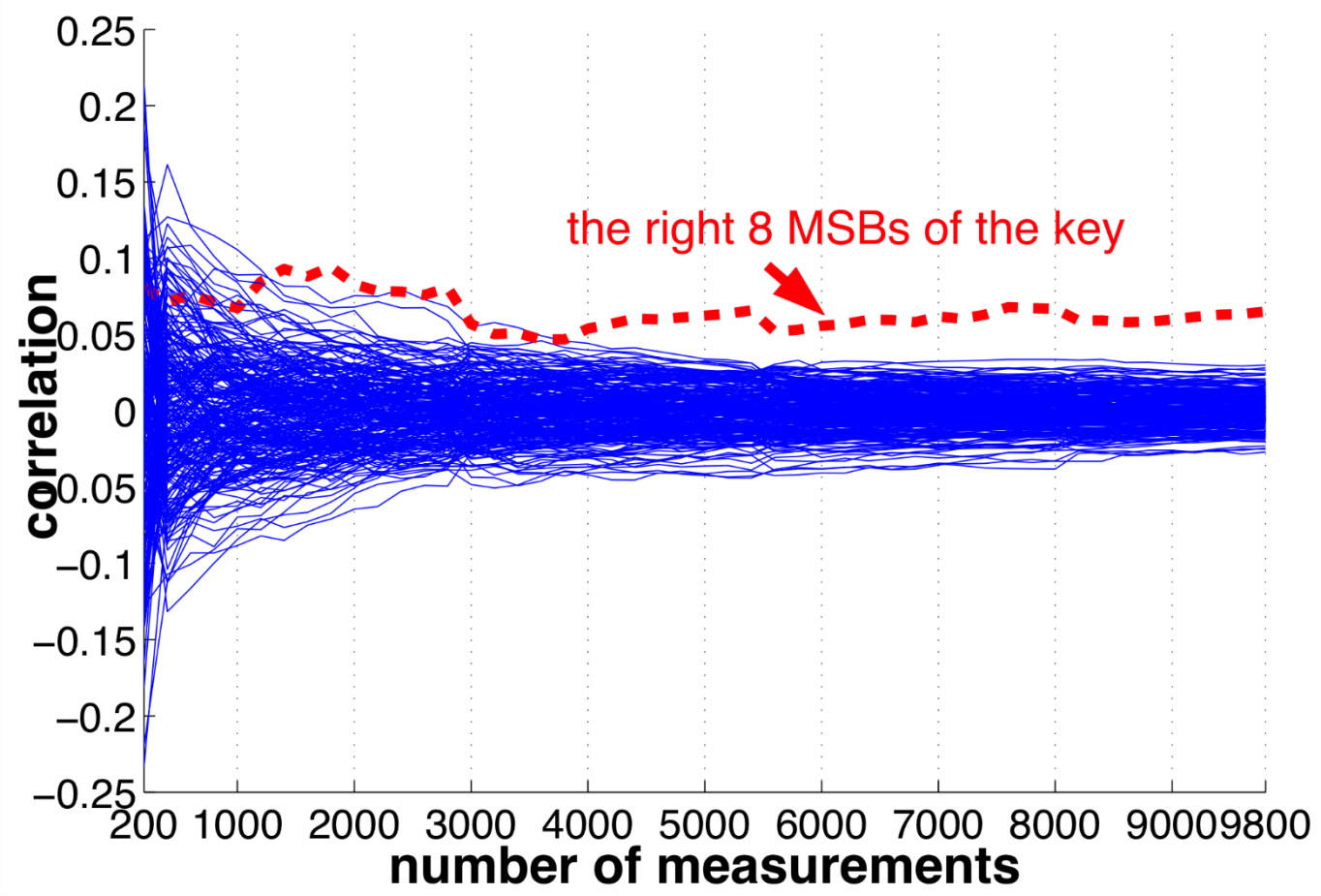


Results of the Correlation Analysis



- The highest correlation occurs at i=153
- This value corresponds to the 8 MSBs of the key.

Finding the required number of measurements



Countermeasures

- Software
  - Time randomization
  - Permuting the execution
  - Masking techniques
- Hardware
  - Increasing the measurement noise by a random number generator (RNG) (Kocher 1999)
  - Power signal filtering (Shamir 2000 and Coron, Goubin 2000)
  - Novel circuit designs
    - Detachable power supplies (Shamir 2000)
    - Logic level (Tiri and Verbauwhede 2003)
    - Asynchronous circuits (Fournier \emph{et. al} 2003)
  - Reversible logic (Golic 2003)

Fault Based Attacks

A successful fault attack requires two steps:

- the fault injection
  - Electrical; Vcc glitch, clock
  - Light-Beam
  - Electromagnetic field
- the fault exploitation
  - Operation system and

  Application sensitive process
  - Cryptographic algorithm