

Power Analysis of Stream Ciphers



Joseph Lano, Nele Mentens,
Bart Preneel, Ingrid Verbauwhede

ESAT/SCD-COSIC

Oct. 15th, 2004. 2.00 pm

Overview

- ➔ ■ Motivation
- Power analysis: Overview
- Power analysis of stream ciphers
 - Irregularly clocked
 - Regularly clocked
- Conclusion

Motivation

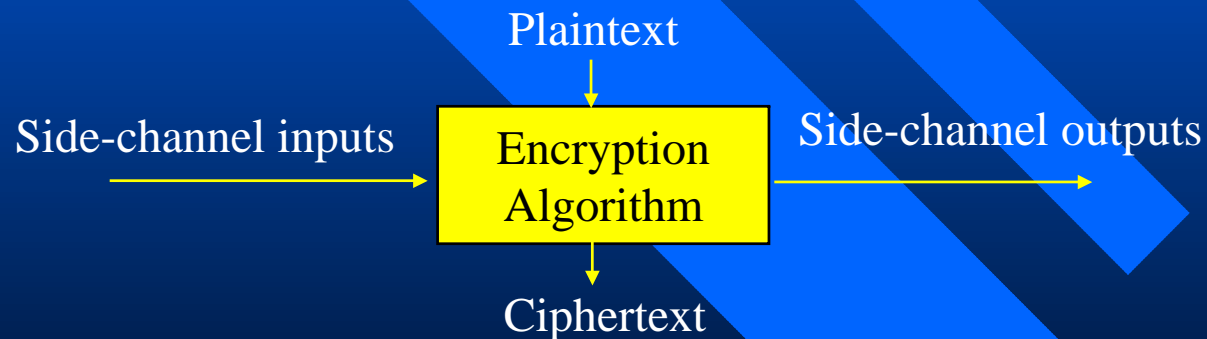
- Side-channel analysis of block ciphers has received much attention.
- Very little research towards the security of stream ciphers against SCA
 - Overview: See previous talk
- Implementation aspects should be taken into account when evaluating stream ciphers

Overview

- Motivation
- ■ Power analysis: Overview
- Power analysis of stream ciphers
 - Irregularly clocked
 - Regularly clocked
- Conclusion

Side-channel attacks

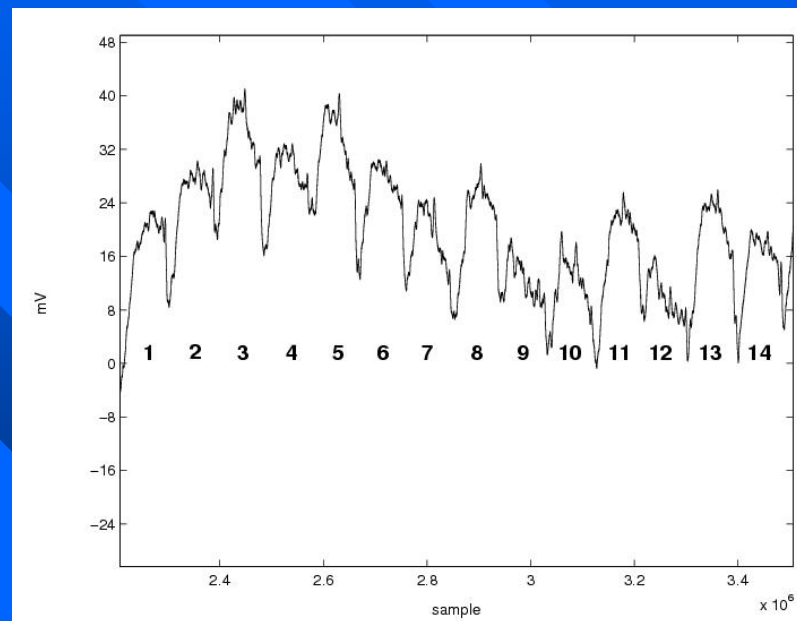
- Cryptanalytic attacks study abstract mathematical model
- Side-channel attacks exploit the implementation of the algorithm



- Active attacks: fault analysis
- Passive attacks: timing, power, EM analysis, ...

Power analysis

- Measure the power consumption during the execution of the algorithm
 - Obtain power trace
- Try to extract the key from trace(s)
 - SPA
 - DPA

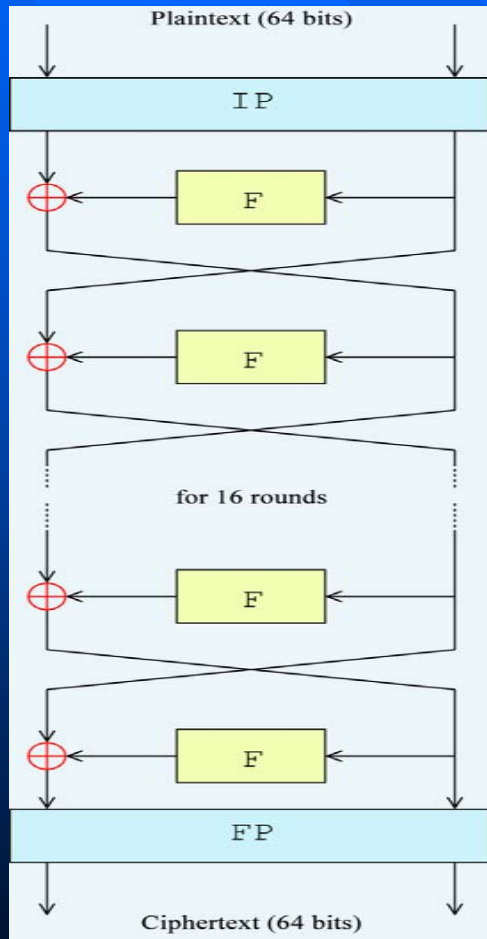


Why does power analysis work?

- CMOS technology: power consumption correlated with:
 - Operations being executed
 - Data being processed
- Often submerged in noise. Hence DPA uses:
 - Many measurements
 - Statistical models

Example: DPA of DES

PB



Phase 1: Power measurement

(P1,C1,T1)

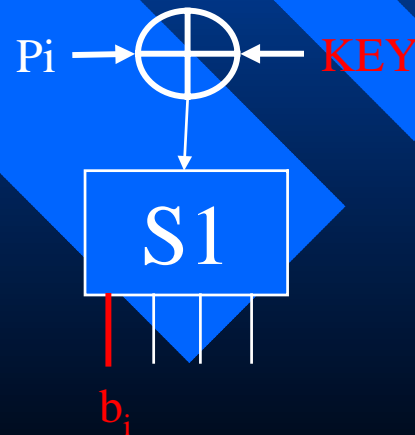
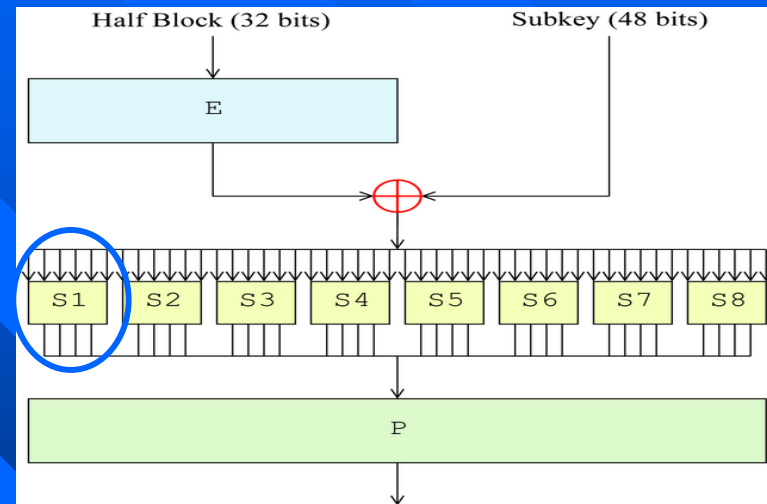
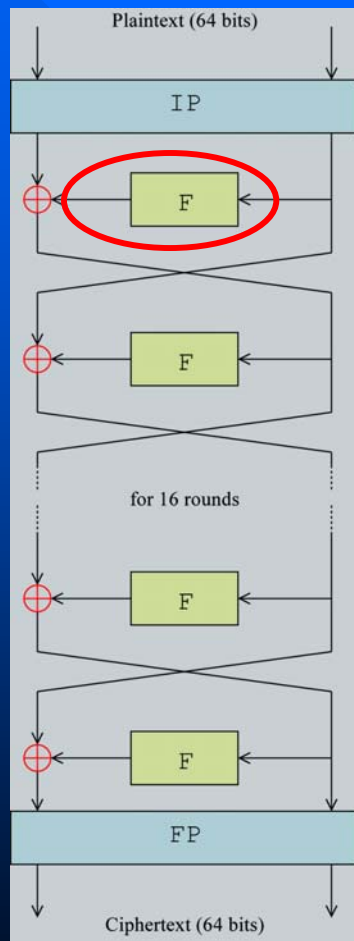
(P2,C2,T2)

(P3,C3,T3)

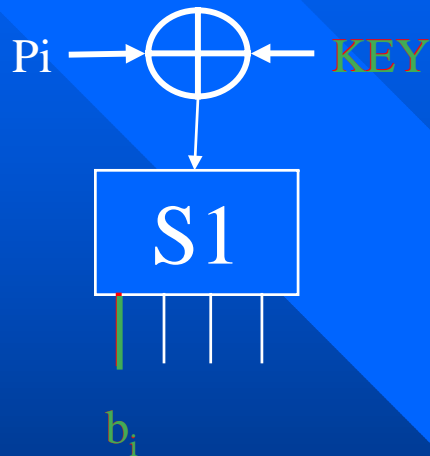
...

CB

Example: DPA of DES (ctd.)



Example: DPA of DES (ctd.)



Phase 2: Extracting key information

- + Key idea: Power consumption of T_i is correlated with the value of b_i
 - + Guess the 6 key bits of KEY
 - + Divide your measurements into two sets V_0 and V_1 as follows:
 - If $b_i = 0$, put T_i into V_0
 - If $b_i = 1$, put T_i into V_1
 - + Compute $H = \text{Meantrace}(V_1) - \text{Meantrace}(V_0)$
 - + If our guess for the key was correct, then :
 - V_0 contains all traces where $b_i = 0$
 - V_1 contains all traces where $b_i = 1$
- Thus H will have a noticeable bias if the number of traces is high enough
- + If our guess for the key was wrong, we divided our measurements into two random sets.

Power analysis

- Many similar attacks exist
 - Against block ciphers (DES, AES candidates)
 - Against public-key cryptosystems (RSA, elliptic curves)
- No attacks against stream ciphers described yet.

Overview

- Motivation
- Power analysis: Overview
- ■ Power analysis of stream ciphers
 - Irregularly clocked
 - Regularly clocked
- Conclusion

Power analysis of stream ciphers

- For a successful DPA attack, you need:
 - Data bits dependent on few key bits
 - Measurements that can be repeated
 - » **Stream cipher is used as one-time pad**
 - Interference of data and key
 - » **In Synchronous stream ciphers, key stream is generated independently from data**
- Extension of DPA attacks to stream ciphers is not obvious.

Power analysis of stream ciphers (ctd.)

- These problems are overcome if the stream cipher has a resynchronization mechanism:
 - A single key encrypts many frames
 - Each frame will be a power trace
 - The known IVs act just like plaintext

Overview

- Motivation
- Power analysis: Overview
- Power analysis of stream ciphers
 - ➔ – Irregularly clocked
 - Regularly clocked
- Conclusion

Irregularly clocked stream ciphers

- Number of operations executed in a clock is dependent on the key
 - Easy to mount a power analysis attack
- Number of traces needed can be expected to be quite low

Ex.: attack on A5/1

- Similar to the attack on DES
 - Collect a number of traces
 - 3 key bits determine whether 2 or 3 LFSRs are updated at $t=86$
 - Guess these 3 key bits and divide measurements into two sets.
 - The correct value for the key bits is the one for which the difference between the two sets is the largest.
 - Go to the next clock to recover more bits of the key

Overview

- Motivation
- Power analysis: Overview
- Power analysis of stream ciphers
 - Irregularly clocked
 - – Regularly clocked
- Conclusion

Regularly clocked stream ciphers

- Power analysis based not on the operations, but only on the data being processed:
 - Stronger requirement, more measurements will be needed.
- We need an adequate consumption model for the implementation, e.g.:
 - Hamming weight model
 - Linear model

Ex.: attack on E0

- Similar to the attack on DES
 - Collect a (large) number of traces
 - 4 key bits determine the hamming weight of the inputs to the output function at $t=0$ (level 1)
 - Guess these 4 key bits and divide measurements into five sets (hamming weight 0 to 4).
 - The correct value for the key bits is the one for which the differences between the sets are the largest.
 - Go to the next clock, update the blender, and continue to recover more bits of the key

Overview

- Motivation
- Power analysis: Overview
- Power analysis of stream ciphers
 - Irregularly clocked
 - Regularly clocked
- ➔ ■ Conclusion

Conclusion

- Power analysis is an issue for stream ciphers with resync.
 - Both for irregularly and regularly clocked
 - Threat is bigger for irregularly clocked
- Research is needed towards the security of stream ciphers against SCA
 - Assessment of the risks by implementing attacks (work-in-progress)
 - Countermeasures against these attacks