Power Analysis Attacks

Elisabeth Oswald

Computer Science Department
Crypto Group
eoswald@cs.bris.ac.uk
Elisabeth.Oswald@iaik.tugraz.at

University of BRISTOL

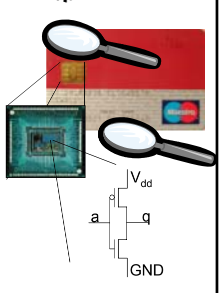
Outline

- Working principle of power analysis attacks
- DPA Attacks on unprotected implementations
- Countermeasures
  - Masking
  - (Hiding)
- Second-order DPA attacks, and template-based DPA attacks on protected implementations
- Comparison, further reading

The goal of this talk is to look into different flavors of DPA attacks.

Power analysis attacks

CMOS technology is the predominant technology for (cryptographic) devices



CMOS Inverter

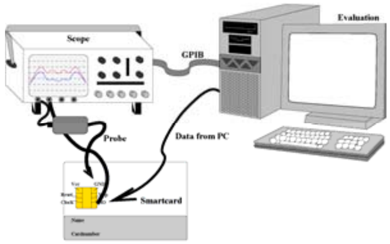
Power analysis attacks exploit the fact that the instantaneous power consumption of a device built in CMOS technology depends on the data it processes and the operations it performs.

Measuring power

- Cryptographic device (device under attack)
- Measurement circuit, probe
- Oscilloscope
- PC

PC configures oscilloscope and sends commands to the device

Oscilloscope records the traces and sends them upon request to the PC



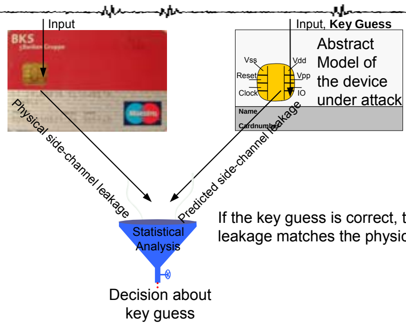
Simple power analysis

SPA attacks are not simple attacks:

- worst case: single-shot
- derive key from very few traces
- often require detailed knowledge about the device and the implementation
- often require sophisticated statistical techniques
- with and without characterization of device

SPA attacks exploit key-dependent differences that occur within a trace. During the attack, there are only very few power traces available.

Differential Power Analysis (DPA): correlation between predicted power consumption and actual power consumption



If the key guess is correct, then the predicted leakage matches the physical (measured) leakage.

DPA attacks exploited key dependent difference that occur in different traces. During the attack, there are typically many traces available.

Template-based DPA attacks

A template attack consists of two phases.

Characterization Phase:
Determine those points that have the most "relevance" and build templates from them:

- A template is built for each intermediate value that can occur
- A template consists of the pair (m,C) that defines multivariate normal distribution.

Analysis Phase:
Match the templates to the given trace(s). The template that fits best, indicates the correct key.

- For each key guess and each input, compute the intermediate value and look up the corresponding template
- The template that fits best indicates the intermediate value and therefore the key.

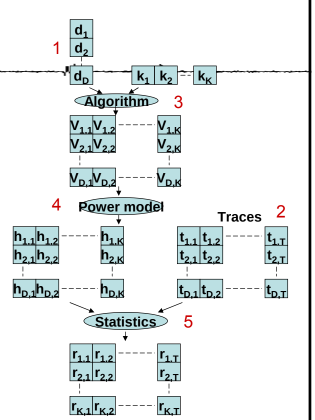
Outline

- Working principle of power analysis attacks
- DPA Attacks on unprotected implementations
- Countermeasures
  - Masking
  - (Hiding)
- Second-order DPA attacks, and template-based DPA attacks on protected implementations
- Comparison, further reading

The goal of this talk is to look into different flavors of DPA attacks.

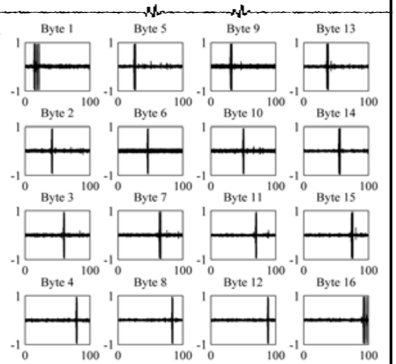
DPA – Step by step

1. Select intermediate result
2. Acquire power traces
   - Different plaintexts, same key
3. Calculate intermediate values
   - Key hypotheses, algorithm
4. Calculate hypothetical power consumption
   - Power model
5. Comparison
   - Statistics



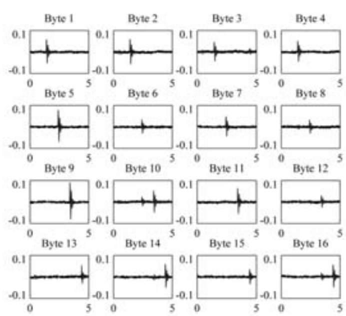
DPA attacks reveal keys and implementation details!

- High correlations indicate correct key byte
- Correlations in this example are almost maximal
- 30 traces are sufficient to reliably determine the key
- Position of DPA peaks reveal the point in time when attacked intermediate result is computed.



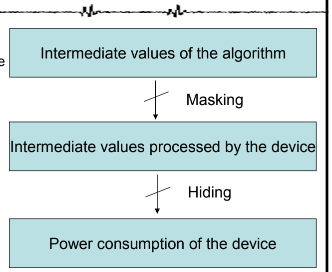
DPA attack on an AES hardware implementation

- DPA peaks reveal information about the key and the implementation
  - Parallelism
- DPA peaks are significantly smaller than for software implementation
- DPA peaks are different for different key bytes



Countermeasures

- Masking
  - Randomize intermediate values of the algorithm
- Hiding
  - Randomize the execution of the algorithm
  - Change the power consumption characteristics

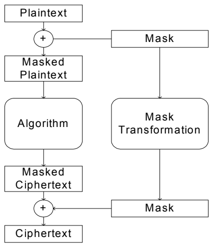


The goal of countermeasures against DPA attacks is to make the power consumption of the cryptographic device independent of the intermediate values of the executed cryptographic algorithm.

Masking

Device with no built in countermeasures + A masked implementation of a cryptographic algorithm = Protected device

© American Express



© Cryptography Research

Goal is to make the intermediate values that are processed by the device independent of the intermediate values of the algorithm

Second-order DPA attacks

- Masking provides security against first-order DPA attacks, if each masked intermediate value v_m is pair wise independent of v and m
  - v_m and m are independent, v_m and v are independent, but
  - v_m and (v,m) are not independent
- Second-order DPA attacks exploit the joint leakage of two intermediate values that are processed by the cryptographic device
  - Any two values u and v that are concealed by the same mask can be used
  - Several of such values typically occur in an implementation for performance reasons

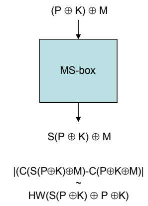
Practical application to masked implementations—Simplified (1-bit) scenario

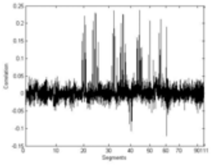
a_m	b_m	HW(a XOR b)	$\|HW(a_m)-HW(b_m)\|$	$\|C(a_m)-C(b_m)\|$
0	0	0	0	0
0	1	1	1	ε
1	0	1	1	ε
1	1	0	0	0

- Second-order DPA attacks work because HW(a XOR b) correlates with a function that can be defined on the traces
  - $|C(a_m)-C(b_m)|$ is a good choice if a device leaks the Hamming weight
  - On 8-bit processors, the correlation can be expected to be about 0.24
  - "Find" $C(a_m)$ and $C(b_m)$ by brute-force search of an "interesting interval"
    - The so-called "pre-processing" step

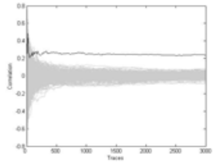
Practical second-order DPA attack on an AES software implementation

- 2nd-order DPA attack:
  - Pre-Processing Step: compute |(C(S(P⊕K)⊕M)-C(P⊕K⊕M)|
  - DPA Step: correlate pre-processed traces with hypothetical power consumption values HW(S(P ⊕K) ⊕ P ⊕K)





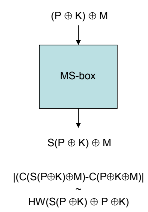
Plot for the correct key



Peak over Traces for all keys

The number of needed power traces can be determined before the actual attack is performed

- We can compute the number of measurements needed for breaking a masked AES implementation
  - We can compute the exact correlation coefficient
    - We simply run through all values of P, K and M (all 8-bit values)
    - It turns out that ρ is 0.2405
- The sampling distribution of the correlation coefficient allows deriving the number of needed traces
  - Transform ρ to a value Z which is normally distributed
  - Use standard methods of statistics to derive N given a ρ and a confidence level 1-α
  - Scale by the SNR of the device
- The number of measurements for ρ = 0.24 is N = 462 ($Z_{0.999}$=3.7)



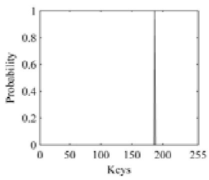
$$N = 3 + 8\left(\frac{Z_{1-\alpha}}{\ln\frac{1+\rho}{1-\rho}}\right)^2$$

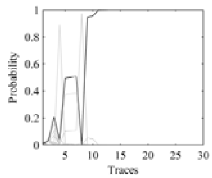
Attacking masking using template-based DPA attacks

Characterization Phase:
- Determine the interesting points with a DPA attack
  - Assume that masks are known during this phase
- Prepare templates that exploit the joint leakage of two intermediate values
  - One template for each pair HW(M), HW(S(P XOR K) XOR M)

Analysis Phase:
- For each key guess and each input, guess all values of M, fetch the corresponding templates and do the template matching
  - p(t|k,M) and p(t,k)=Σ p(t|k,m)
- Use Bayes' theorem to derive p(k|T)

Practical template-based DPA attack on an AES software implementation





- 81 templates
  - Full and reduced templates, using less than 10 interesting points
  - Number of traces for characterization about 10000 (works also with fewer traces)
  - Performance of templates almost optimal (very low error rate)
- Attack succeeds with about 15 traces

Comparison of attacks

- Software (8-bit devices)
  - Unprotected
    - Template: 15 traces
    - DPA: depending on power model and hypothesis: 30-200 traces
  - Protected by masking
    - Template: 15 traces
    - Second-order DPA: depending on power model and hypothesis: 450 – more traces
  - Protected by masking and hiding
    - As least as many as just for masking and more depending on the number of dummy operations, and the way the intermediate values can be shuffled
- Hardware (32-bit architecture)
  - Unprotected
    - Highly depends on the power model: “10000” – and more traces
  - Protected
    - Highly depends on the power model: “10000” – and more traces

Further reading

- “Differential power analysis” – the classic paper by CRI
- Dozens of papers on SPA applied to asymmetric stuff
  - ECC-type, RSA-type systems lead to different SPA issues
- Profiling
  - Little research done
  - Reverse engineering even less
- Template and Collision attacks
  - Read the IBM papers
- Classical cryptanalysis
  - If SPA reveals only some bits, often classical cryptanalysis can do the rest
- The must read: our DPA book
  - Visit: www.dpabook.org