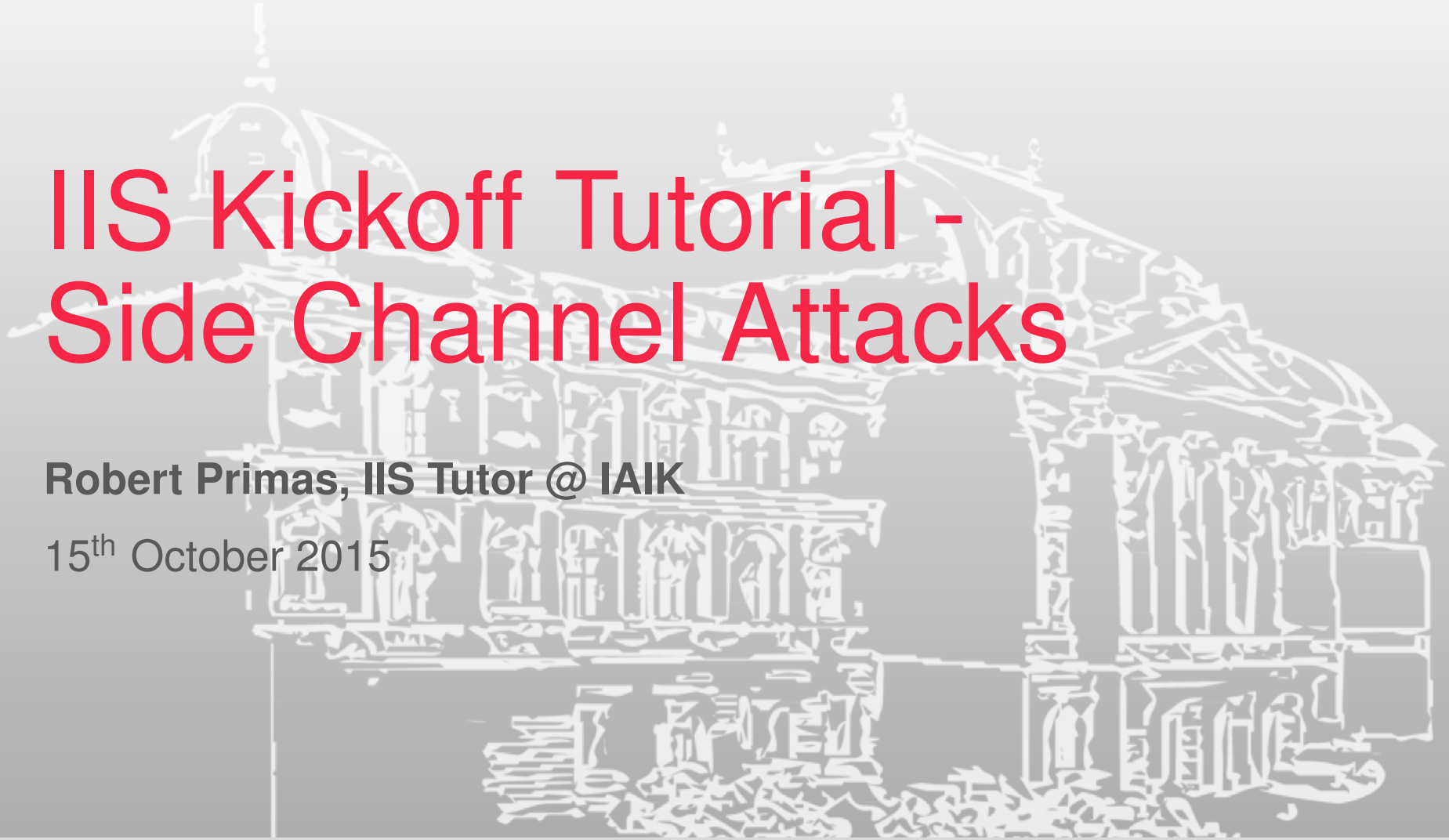


IIS Kickoff Tutorial - Side Channel Attacks

Robert Primas, IIS Tutor @ IAIK

15th October 2015

Content

1. Organisatorial Information
2. Project Specification
3. AES Introduction
4. Side Channel Attacks
5. Submissions
6. Grading
7. Timeline

Tutorials

No weekly tutorials, support directly from Tutor

- Newsgroup (interesting for everyone)
- Email (small problem, interesting for your group)
  - rprimas@student.tugraz.at
  - stefan.steinegger@student.tugraz.at
- Meeting (bigger problem, interesting for your group)
  - Contact tutor for arrangement

Tutorials

Second tutorial will be announced

- Content is advanced Fault Attack
- After group meetings and project specification submission

Tutorial slides will be available on the wiki

Language

IIS Practicals are also in English

- English is appreciated
- German is also ok (oral/written)

Project Specification

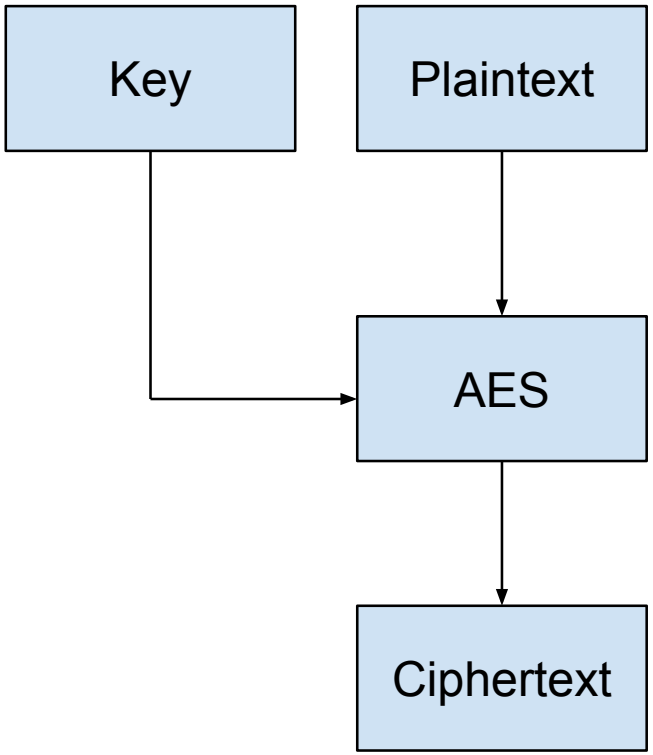
2-4 Pages, describe your problem solving proposals

- Format is PDF
- One specification per group
- Hand in by 17.11 via Stics
- Implement and hand in simple Fault Attack by 17.11 (not mandatory but highly recommended!)

Advanced Encryption Standard (AES)

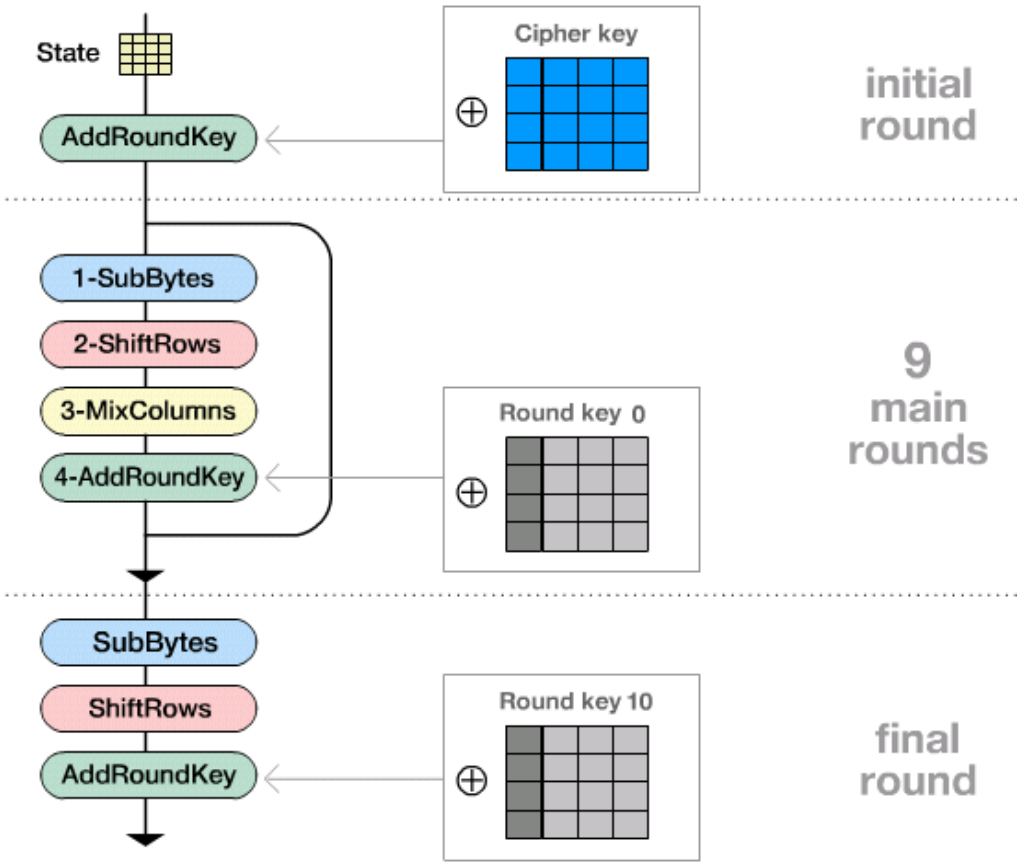
- Symmetric Encryption Scheme
- Data processed in 128 bit blocks
- Key length is **128**, 196 or 256 bit
- Nowadays used almost everywhere
- License Free
- Software/Hardware Implementations

AES Interface



AES Rounds

Animation → https://youtu.be/mlzxpkdXP58



©http://www.kubieziel.de/blog/archives/937-Wie-AES-funktioniert.html

Side Channel Attacks

Two challenge chapters

1. Differential Power Analysis Attack
2. Fault Attacks
    - Simple Attack
    - Advanced Attack

You need to implement all tasks for a good grade

Differential Power Analysis (DPA)

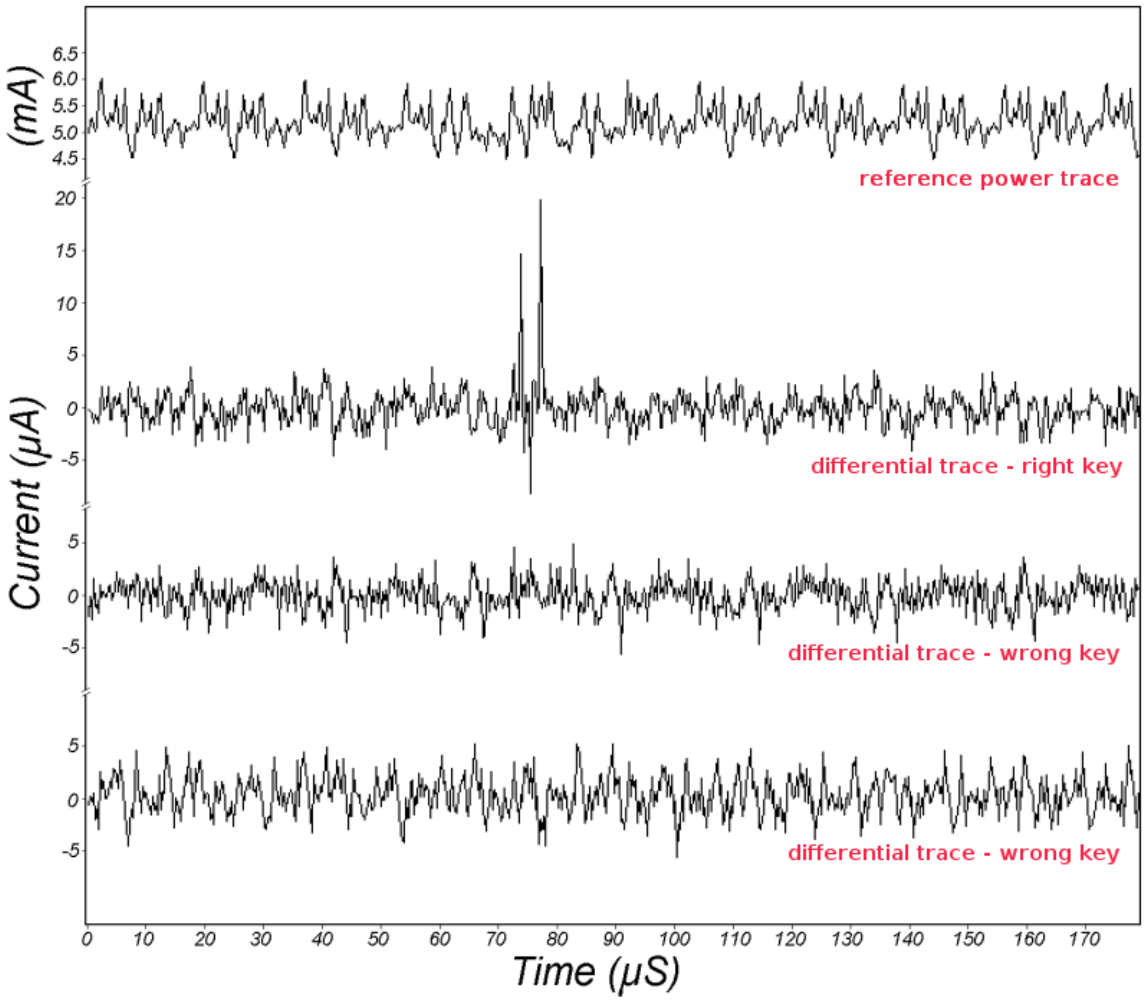
In a nutshell...

- Observation: Power consumption of hardware depends on data values (Key!)
- Make assumptions about the influence of key bits on the power consumption $\rightarrow$ Power Model
- Guess part of key, predict power consumption and look for similar patterns in the recorded power traces $\rightarrow$ Correlation Analysis

DPA - Power Models

- CMOS circuits consume power only when switching states
- Assume high power consumption if the Hamming Weight of the output of the first Subbox is high and vice versa
- Key is right if the predicted power consumption is retrievable from the provided power traces

DPA - Power Traces Example



©http://web.cse.msstate.edu/~ramkumar/DPA.pdf

DPA - Submissions

For Specification

- Short description of the AES cipher
- How would you implement this attack?

For Final Delivery

- Implement a DPA Attack on plaintexts/power traces provided by us (handed out after group meetings)

DPA - References

- Paper: DPA on DES/AES etc.
  `http://link.springer.com/article/10.1007%2Fs13389-011-0006-y`
- Youtube: DPA on DES
  `https://youtu.be/gbqNCgVcXsM`
- Correlation Power Analysis
  `http://www.engr.uconn.edu/~tehrani/teaching/tcs/cpa_shi.pdf`

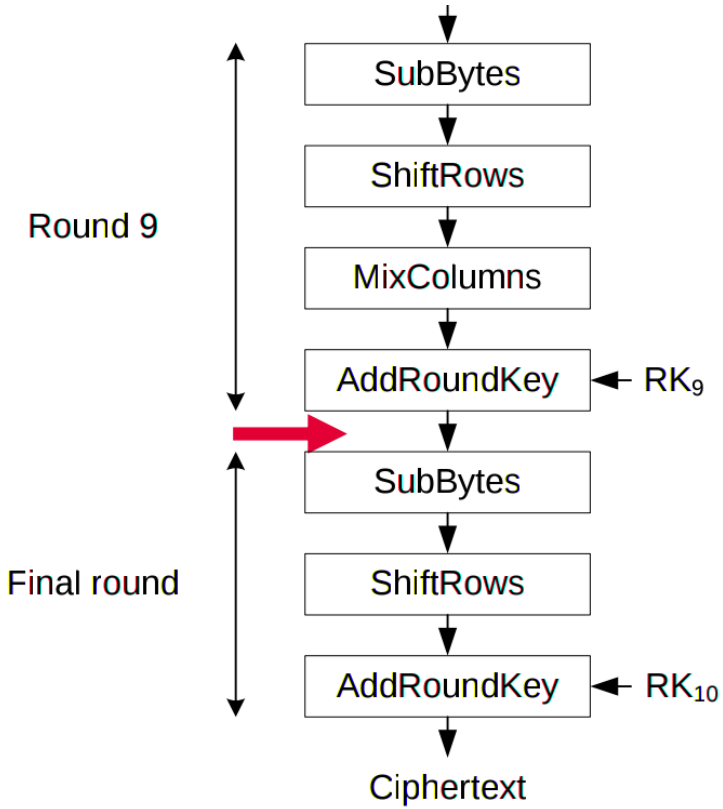
Fault Attacks

In a nutshell...

- Assume ability to induce faults during AES encryption
- Recover key bits from valid/invalid ciphertext pairs

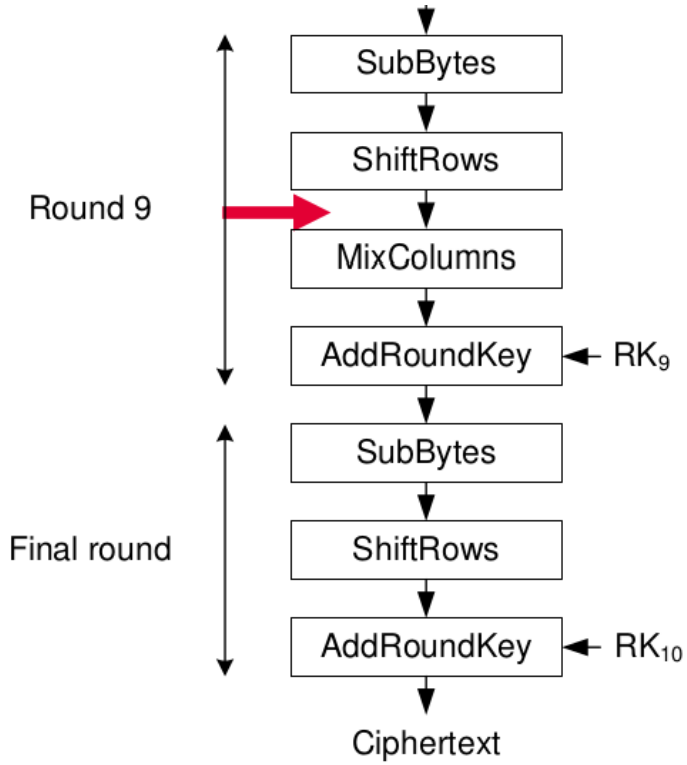
Simple Fault Attack

- Induce bit flip before the last Subbox operation at known position
- Collect valid/invalid ciphertext pairs
- Calculate back to input of last Subbox with guessed key bits
- Find out if the right key was guessed...



Advanced Fault Attack

- Not yet ...
- Is covered in a second tutorial (will be announced)



Fault Attacks - Submissions

For Specification

- How would you implement the simple Fault Attack?
- Recommended: Implement simple Fault Attack

For Final Delivery

- Implement simple Fault Attack
- Implement advanced Fault Attack

Submissions

- Programming language is Matlab/Octave or Sage
- Add Readme with instructions if necessary
- We need to be able to run your code
- Write summary for each solved challenge
  (2-4 Pages in total)

Grading

- Points are earned at the final interview for explaining your correctly implemented attacks
- All group members get same grade (except corner cases)
- All tasks need to be solved for a good grade
- All group members need to be able to explain all implemented attacks

Timeline

- Next days - Handout of simple Fault Attack assignment
- 17th November
  - Send signed rule confirmation email
  - Hand in Project Specification
  - Hand in simple Fault Attack (recommended, not mandatory, no support after this date)
- $\sim$ 23th November - Group Meetings
- $<$ 24th December - Give progress update to tutor
- 21th January - Final deliverable
- $\sim$ 28th January - Final interviews