

# Cryptography and Embedded System Security

## CRAESS\_I

Xiaolu Hou

Slovak University of Technology  
xiaolu.hou@stuba.sk

# Time table

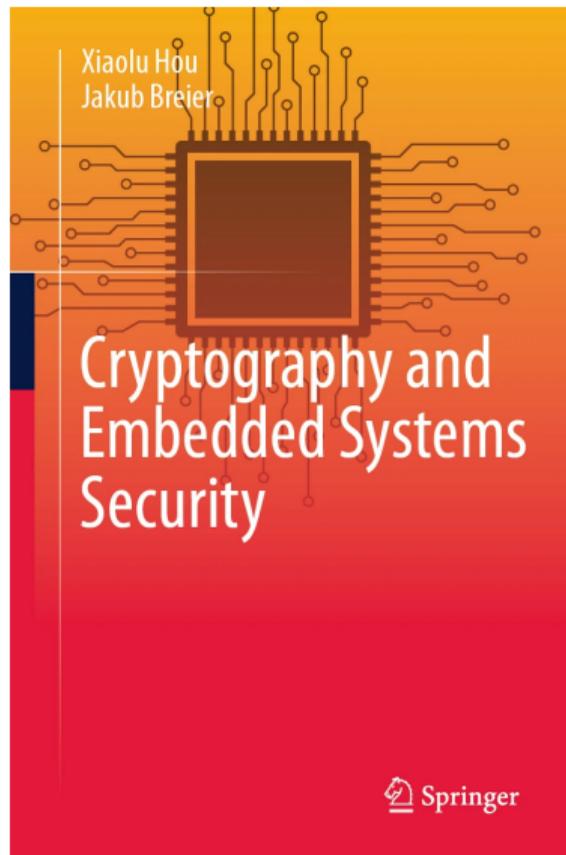
- Lectures (prednášky)
  - Friday 10 – 11:50
- Tutorials (cvičenia)
  - Friday after the lecture
  - 12 – 13:50
- Consultations (konzultácie)
  - By appointment, [xiaolu.hou@stuba.sk](mailto:xiaolu.hou@stuba.sk)
  - Office 4.03

# Grading

- 50 marks – six assignments
  - Assignments with questions
    - Solution to be written with latex, submission of PDF in AIS
  - Programming assignments
    - Submission of code in AIS
    - Individual presentation of implementation details
    - Assignments 4 and 5 also require short answers for a few questions to be submitted in PDF in AIS
  - 0 grade for late submission
- 10 marks – quiz
- 10 extra marks
  - Find mistakes in textbook
- 40 marks – final exam
  - To sit in the final exam, you should obtain at least 30 marks during the semester

## Textbook

- Cryptography and Embedded Systems Security
- Springer link:  
<https://link.springer.com/book/10.1007/978-3-031-62205-2>
- Free version: <https://xiaoluhou.github.io/Textbook.pdf>
- Library: 6 copies, I\*6K-Kryptografia, šifrovanie



## Mistakes in the book

- 1 mistake – 1 mark
- At most 10 marks in total
- Mistakes, grammar errors, confusing sentences, etc
- Report mistakes: in team group message, email, or just talk to me
- Only newly found errors will be awarded marks
- Errors identified during the lectures do not count
- Up to date version: <https://xiaoluhou.github.io/Textbook.pdf>
- Errata: <https://xiaoluhou.github.io/Errata.pdf>

# Attendance

- Mandatory tutorials
  - Week 4: presentation of Assignment 3
  - Week 9: presentation of Assignment 4
  - Week 10: presentation of Assignment 5 solution
  - Lectures might end early, so better come at least half an hour before the tutorial starts
- Week 6: Quiz, 10-11:50am, lecture will be after quiz
- If cannot attend, a valid excuse note should be submitted, otherwise **0 marks**

## Course materials

`https://xiaoluhou.github.io/Teaching\_material/`

or

`https://github.com/XIAOLUHOI/Teaching\_material`

## Note

- Some lectures might be online - pay attention to announcements in teams group chat and emails

# Datasets and analysis code for SCA

All datasets and analysis code related to SCA can be found here

```
https://github.com/XIAOLUHOU/  
SCA-measurements-and-analysis----Experimental-results-for-textbook/  
tree/main
```

## Extra reading materials

- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.
  - Free online: <https://cacr.uwaterloo.ca/hac/>
- Stinson, Douglas R. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.
  - Free online: [http://sutlib2.sut.ac.th/sut\\_contents/H97066.pdf](http://sutlib2.sut.ac.th/sut_contents/H97066.pdf)
- Lecture notes, Hardware and Embedded Systems Security, <https://creativecommons.org/licenses/by-sa/3.0/>
- Buchmann, Johannes. Introduction to cryptography. Vol. 335. New York: Springer, 2004.
- Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.
- EC council course, <https://codered.eccouncil.org/course/cryptography-and-embedded-systems-security?logged=true>



## Why are we interested in physical attacks?

- Cryptography provides algorithms that enable secure communication in theory
- In the real world, these algorithms have to be implemented on real devices:
  - software implementations: microcontroller
  - hardware implementations: FPGA
- To evaluate the security level of cryptographic implementations, it is necessary to include a physical security assessment

# Targets and Attack Goals

## Targets

- Credit cards
- Passports
- Key Fob
- ...

## Goals:

- Recovery of the secret key
- Privilege escalation
- IP theft
- ...



# Different Physical Attack Methods

- Side-channel analysis attacks
  - EM/Power analysis
  - Timing analysis
  - Cache attacks
- Fault attacks
  - Optical fault injection
  - Electromagnetic fault injection
  - Clock/voltage glitch
- Hardware Trojans
- ...



# What will we cover in this course?

- Abstract algebra and number theory (week 1)
- Introduction to cryptography (week 2)
- Modern cryptography and implementations (week 3 – 4)
- Power analysis attacks, fault attacks, and countermeasures (week 5 – 11)
- Practical aspects of physical attacks (week 12)
  - Invited speaker, Dr. Jakub Breier, Senior security manager, TTControl GmbH
- Consultation (week 12) – most exam questions will be from examples during the lectures

## An important notation

- Decimal point is denoted by . not ,

$$\frac{1}{2} = 0.5$$

- We do not use

$$\frac{1}{2} = 0,5$$

- Ten thousand is written as 10,000
- If there are more confusing notations for you, do let me know!

# Master and PhD topics

- Fault attacks and countermeasures
  - Cryptographic implementations
  - Neural networks
- Side-channel analysis attacks and countermeasures
  - Cryptographic implementations
  - Neural networks
  - AI for side-channel analysis attacks
- You are highly encouraged to continue your master's or Ph.D. studies with me
- You will have a good starting point for your research after finishing this course
- Later parts of the course are based on recent publications