Advanced Topics in Security: Side channels – from theory to practice

236652

Lecturer: Prof. Debdeep Mukhopadhyay, IIT Kharagpur

Lecturer in charge: Prof. Avi Mendelson

2 credit points

Feb 20-21, 24-26, 2019

This course will focus on understanding the different security threats on modern hardware design with special emphasis on side channel related aspects. In particular, the course will focus on basics of hardware design for cryptographic algorithms, emphasizing on AES (Advanced Encryption Standard), and ECC (Elliptic Curve Cryptography), as representatives for symmetric key and asymmetric key ciphers. The course will also discuss the following topics: techniques on finite fields, which have been used to develop efficient primitives, like S-Boxes, Finite Field multipliers and inversion circuits. Side channel attacks that measure power consumption. Detailed treatment starting from the basics to state-of-the-art statistical analysis would be presented. Evaluation criteria for side-channel secured products, in particular combination of common criteria and FIPS styles. Usage of fault analysis for cryptanalyzing ciphers, like AES. State-of-the-art techniques like Differential Fault Intensity Attacks (DFIA), which can be used to break conventional fault tolerance techniques. The course shall subsequently delve into the topic of micro-architectural attacks, focusing on topics like cache attacks, branch predictor attacks, and row-hammer attacks. Finally, it will discuss countermeasures against the side-channel analysis (e.g., against power and fault analysis).

The course will be taught in English

Syllabus:

Hardware for Cryptography; Finite Field Hardware Design; Hardware Design of AES; Hardware Design of Elliptic Curve Crypto; Compact Design of AES S-Box, Side Channel Analysis, Power Analysis, Fault Analysis, Kocher's Timing Attacks, techniques for Differential Power Attacks, Test Vector Leakage Assessment, Side Channel Robustness Testing: Common Criteria vs FIPS, Fault Analysis of Cryptosystems, DFA on AES with single faults, Diagonal Fault Attacks, Differential Fault Intensity Attacks, Fault Analysis Automation., Micro-architectural Attacks: Cache Attacks, Branch Prediction Attacks, RowHammers, Countermeasures: masking, Threshold Countermeasures, Fault Attack Counteremeasures: detection vs infection.

Learning Outcomes:

At the end of the course, the student will be abreast of hardware designs of complex cryptographic algorithms, and shall be able to map them into efficient hardware architectures. The student shall also be able to develop novel side-channel analysis of crypto designs, coupled with thorough understanding of the cause of such attacks. The course will enable the student to evaluate cryptosystems wrt. Side channel analysis and design suitable safeguards. It is expected that the course shall provide a sound background to the student to perform research in the field of Hardware Security.

Text Books:

- Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press

Reference Books:

- Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
- Ted Huffmire et al: Handbook of FPGA Design Security, Springer.
- Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007.
- Doug Stinson, Cryptography Theory and Practice, CRC Press.

Grading:

50% Drills, Problem Sheets, and 50% final work

Detailed syllabus is below:

There may be some deviations from this plan.

Topic #	Time (in mins)	Lecture	Tutorial	Assignment
1	60	Introduction to Hardware Security		
2	45	Algorithms to Hardware		
3	50	Finite Field Architecture		
4	50	Hardware Design for Finite Field Inverse		Drill on S-Box
5	35	Background on Cryptography, Cryptanalysis and Advanced Encryption Standard (AES)	Problem Sheet-I	
6	30	AES and Cryptanalysis		
7	60	Field Isomorphism		

8	90	Hardware Implementation of AES		
9	50	Compact AES S-Box		
10	55	Compact AES S-Box in Normal Basis	Problem Sheet-II	
11	120	Hardware for Elliptic Curve Cryptography		
12	30	Introduction to Side Channel Analysis		
13	60	Differential Power Attack and Difference of Mean		
14	30	Power Setup and Power Model		
15	30	Statistics and Power Analysis	Problem Sheet-III	
16	60	Correlation Power Analysis, Mutual Information Analysis		Drill based on Power traces
17	60	Common Criteria and FIPS for Certification		
18	30	Introduction to Fault Analysis		
19	60	Differential Fault Analysis on AES		Drill based on DFA
20	30	Differential fault intensity analysis	Problem Sheet-IV	Drill based on DFIA
21	30	SIFA		
22	60	Algebraic Fault Analysis		
23	60	Automation of Fault Analysis		
24	60	Cache Attacks: Trace, Access, Timing		
25	30	Leakage due to Hardware Prefetchers	Problem Sheet-V	
26	60	Branch Predictor Unit Attacks		
27	30	RowHammer		

28	30	Countermeasures: Masking and Glitches		
29	30	Threshold Implementation	Problem Sheet-VI	
30	60	Redundancy, Infective Countermeasures, Fault Space Transformation		

The course is plan to take place on the 20.2 -21.2 and continue 24.2 – 26.2