Final Projects

EEE5716/EEE4714: Introduction to Hardware Security and Trust

Fall 2025

Deadlines

- December 8, 2025, 11:59 pm (Subject to change): Final project report and other deliverables are due.
- During finals week, TAs may reach out for a project demonstration by appointment, depending on the project and our ability to replicate your results.

Important Points

- If your project requires any additional hardware (excluding the FPGA board), your team is responsible for purchasing the hardware and splitting costs.
- Source files (programming scripts, RTL, etc.) must be commented on and cleanly written. They are graded as part of your report.
- The ECE Linux server can provide licensed software tools (Synopsys Design Compiler, IFV, Jasper). Xilinx Vivado is free to download on your personal computer. Refer to vnc_setup_and_tools_access.pdf in Canvas for help accessing the ECE Linux server.
- **Start early.** Except in extenuating circumstances, extensions will not be granted. TAs may help debug tooling problems during office hours, but we will certainly be flooded with such requests close to the project deadlines and unable to help everyone.
- If your project is not working or your results are not as clean as you had hoped, this does not mean you will get a bad grade. In this scenario, focus on writing a detailed, high-quality report on what works. Explain where you suspect problems occurred and how you would try to fix them.

6 Side-Channel Attacks on Advanced Encryption Standard (AES)

Main Objective In this project, you will extract the key to an Advanced Encryption Standard (AES) cryptographic algorithm through a side-channel attack using power analysis, with as few as possible collected power traces.

Background In cryptography, a side-channel attack is based on information gained from the physical implementation of a cryptosystem rather than brute force or theoretical weaknesses in the algorithms (in contrast with cryptanalysis). For example, timing information, power consumption, electromagnetic emanations, or even acoustic sound can provide an extra source of leaked information, which can be exploited to break the system. Some side-channel attacks require technical knowledge of the internal operation of the system on which cryptography is implemented. However, others, such as differential power analyses, are effective as black-box attacks. Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher.

Power analysis is a form of side-channel attack in which the attacker studies the power consumption of a cryptographic hardware device (e.g., smart card, tamper-resistant "black box", or integrated circuit). The attack can non-invasively extract the device's cryptographic keys and other secret information. Simple power analysis (SPA) involves visually interpreting power traces or graphs of electrical activity over time. Differential and Correlation power analysis (DPA/CPA) are more advanced forms of power analysis that can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations.

Project Goal: The students must mount a DPA/CPA attack on the public power traces provided in the DPA contest v2 (https://www.dpacontest.org/v2/download.php). Students should optimize their algorithm to obtain the key with as few power traces as possible.

Overall Requirements: For this project, you need to implement a DPA/CPA on power traces that were collected from an AES module (https://www.dpacontest.org/v2/data/aes_dpa_contest_v2.tar.gz). You can download these traces from the public database: https://cloud.telecom-paris.fr/s/N5qgyMdxEcqipN2.

1. There are 640,000 AES traces of 32 different keys, as presented in the public database. Each key has 20,000 encryption traces with random plaintexts. Keys and plaintexts can be found in the index file[1].
2. For four keys in the data set, target the corresponding traces using your CPA/DPA attack scripts and report your results.

Keys	082efa98ec4e6c89452821e638d01377	be5466cf34e90c6cc0ac29b7c97c50dd
		00000000000000003243f6a8885a308d3
		13198a2e03707344a4093822299f31d0

Table 1: Specified keys

3. Randomly select two additional keys and report whether your scripts successfully extract those keys.
4. Attempt to optimize your code to find the key with as few power traces as possible.

Note that you can find useful materials like reference tools and templates to help you build the attack scripts on this page (https://www.dpacontest.org/v2/download.php).

Software Requirements Scripting language for analyzing/visualizing your results. Python, MATLAB, or others.

Hardware Requirements

None

Report to submit.

- IEEE conference format. (4-6 pages)

[1] https://www.dpacontest.org/v2/data/keymsg_public_base_dpacontest2.bz2

- The report should include (tentative marks dist.):
    1. Top Sheet with group members' names and ID
    2. Introduction, motivation, and problem statement. (10%)
    3. Methods (40%)
        - Describe why you chose either DPA or CPA
        - Describe how your chosen method of power analysis works.
        - Describe how your scripts work.
    4. Results and discussion (35%)
        - Do your scripts work for all of the required keys? How did you tweak your algorithms to work for your assigned keys?
        - How many traces do your scripts need to process before they start to reveal correct key byte guesses?
        - Include sample plots for different guesses at round-key bytes and compare the figures of the correct guess with the wrong guesses. The correct guess should be obviously different from the incorrect guesses.
        - *After* tweaking your algorithms, randomly select (UG:1 and G:2) keys other than your assigned ones and report whether your scripts can successfully deduce the key. Include plots as appropriate.
    5. Conclusion & Personal comments (10%)
    6. Clarity, organization, etc. (5%)

Submission guidelines

- Submit a .zip file with name: Project#Group#
- Include all of the following:
    - Report.pdf
    - Working directory for your analysis

      * readme.txt (provide necessary instructions for running your code) *

      All source files.

References

1. https://www.dpacontest.org/v2/index.php
2. Kocher, P., Jaffe, J., Jun, B., & Rohatgi, P. (2011). Introduction to differential power analysis. Journal of Cryptographic Engineering, 1(1), 5-27.
3. Brier, Eric, Christophe Clavier, and Francis Olivier. "Correlation power analysis with a leakage model." International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2004.
4. Clavier, Christophe, et al. "Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest." Journal of Cryptographic Engineering 4.4 (2014): 259-274.
5. Lo, O., Buchanan, W. J., & Carson, D. (2017). Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). Journal of Cyber Security Technology, 1(2), 88-107.
6. Randolph, M., & Diehl, W. (2020). Power side-channel attack analysis: A review of 20 years of study for the layman. Cryptography, 4(2), 15. https://doi.org/10.3390/cryptography4020015.
7. Maghrebi, H., Portigliatti, T., & Prouff, E. (2016, December). Breaking cryptographic implementations using deep learning techniques. In International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 326). Springer, Cham

8. Hnath, William. Differential power analysis side-channel attacks in cryptography. Diss. Worcester Polytechnic Institute, 2010.