Exercise Sheet Week 10

—Side Channel Analysis on Elliptic Curve Cryptography—

Submission deadline: November 18, 2024, 11:30 via Aplus/MyCourses

All exercises study implementations of countermeasures against side-channel analysis. The exercise sheet gives at most 4 points. As usual, you can choose which of the exercises you solve and combine them according to your preferences, e.g., focus only on implementation tasks (Aplus), only on pen-and-paper exercises (MyCourses) or a mix of both. Below are two separate sets of instructions for Ex. 2 & Ex. 4-6 (MyCourses) and Ex. 1 & Ex. 3 (Aplus).

Ex. 2 & Ex. 4-6: Submission as a PDF to MyCourses as in the previous weeks.

Ex. 1 & Ex. 3: You need **Python3**.

Submission via Aplus: `https://plus.cs.aalto.fi/cs-e4340/2024/`

We built some automated graders for Aplus to give you direct feedback on your (up to 10) submissions, but the automated graders are really a beta version. In particular, error messages are rather cryptic, and it might happen that the grader does not give you full points although it should. If you do not get full points on an Aplus exercise, we will check the grading **manually** and **might increase the points later**.

Please **add comments** to explain what your code is doing, this is especially useful if we need to **manually check** it. Each of the exercises only requires writing a few lines of code. We don't commit to manually study long or complicated code, especially without comments.

Exercise 1 (DPA countermeasure 1: Key Randomisation)**.** *2 points, via Aplus*
Task. Implement the key randomisation countermeasure as discussed during the lecture.

Hint: When implementing key randomization, you need to ensure that your randomised key is functionally equivalent to the original key. Reading the questions in Exercise 2 might be inspiring, too.

Exercise 2 (DPA countermeasure 1: Key Randomisation)**.** *2 points, via MyCourses* Which algorithms out of kgen, enc and dec of the El Gamal public-key encryption scheme[1] need to implement key randomization in the key randomization countermeasure? Justify your answer. Explain how to modify the algorithms in question[2] and why to modify them in this way. How would one benchmark *in a machine-independent-way* how an implementation of the key randomization countermeasure affects the algorithm's performance? Discuss what would happen if the parameter for implementing this countermeasure is too small or too large.

Exercise 3 (DPA countermeasure 2: point blinding)**.** *4 points, via Aplus* **Task.** Implement the countermeasure for point blinding as discussed in the lecture.

Exercise 4 (DPA countermeasure 2: point blinding)**.** *4 points, via MyCourses* Which algorithms out of kgen, enc and dec of the El Gamal public-key encryption scheme[3] need to implement point blinding in the point blinding countermeasure? Justify your answer. Explain how to modify the algorithms in question[4] and why to modify them in this way. How much is the overhead induced by this countermeasures using a machine-independent efficiency measure?

Exercise 5 (Comparison)**.** *2 points, via MyCourses* How does the efficiency of the point blinding countermeasure compare to the efficiency of key randomization, i.e., which one slows down the algorithms more?

Exercise 6 (Advanced)**.** *4 points, via MyCourses* Think about possible side-channel attacks that we can expect to be successful in the presence of one countermeasure, but not in the presence of the other. Justify your suggestions. For inspiration, you can come up with your own ideas or do a bit of research on scientific works. This is a research task, i.e., we do not have a model solution for this question.

[1] You can either read the code on Aplus and/or the Wikipedia page on El Gamal `https://en.wikipedia.org/wiki/ElGamal_encryption`

[2] You may refer to your own code here in case you solved Exercise 1 also.

[3] You can either read the code on Aplus and/or the Wikipedia page on El Gamal `https://en.wikipedia.org/wiki/ElGamal_encryption`

[4] You may refer to your own code here in case you solved Exercise 3 also.