Fall 2020 - CS 331 (Microprocessor Systems)

Hardware Security - Assignment 2

The goal of this assignment is to illustrate some of the efficiency and security aspects we discussed in lectures 5 and 6.

Part 1: Montgomery modular multiplication

In lecture 5, we studied how to implement modular multiplication in a way that's friendly to the hardware. Your first task is to modify this RSA implementation to use Montgomery modular multiplication and measure the performance speed up in the decryption process.

Hints / Notes:

- It is possible that you will not observe a speed up at your first attempt. Some changes in how you are using the BigInteger class could be needed.
- While the Chinese Remainder Theorem could also make the performance better, don't use it in the implementation. This is to make the next part easier for you. Note that in practice, RSA implementations are more sophisticated. In this assignment, the code is simplified for the purpose of learning. You should never use this implementation in the real world.

Part 2: Side-channel timing attack

In this part, you will implement a more advanced version of the attack that we discussed in lecture 6. Note that Paul Kocher's attack that we discussed required knowledge about the target hardware. In this assignment, the attack will not require this knowledge.

The attack you will implement is described in Section 3.4 in this paper. The target of the attack is modular exponentiation with Montgomery's multiplication that you implemented in the first part.

Performing the attack to know the full private exponent will be time-consuming, so you will do the following instead:

- Your goal will be to make experiments to verify that the **second most significant bit** of the private exponent given in the above file is one.
- You will experiment with different portions of the given private exponent. For example, in the first experiment, you will assume that the private exponent used by the target implementation is only the three most significant bits. In the second experiment, you will assume that it's only the five most significant bits, and so on.
    - Here are the lengths that you will try {3, 5, 10, 20, 50, 100}. Each number represents the number of most significant bits that the implementation will use as the private exponent.

    - For each of these lengths, you will repeat the experiment for 20 times, and count how many times the result was consistent with the fact that the second most significant bit is 1.
    - In each trial of the 20 repetitions, collect execution times for at least 10000 samples, and then proceed as described in the paper to know whether the second most significant bit is 0 or 1. If the technique outputs 1, then it's a success, otherwise, it's not.

Hints:

- You don't have to understand all the formal details in the above paper.
- To make the attack more feasible and easier to observe, you can **amplify** the timing difference in the branch in Montgomery's algorithm. For example, instead of doing the subtraction once, you can repeat the subtraction for a few more times without affecting the correctness. (Make sure to do that after collecting the speed-up measurements needed for part 1)
- Note that the attack has some similarity to the differential power analysis attack. You collect measurements in the first stage, and then you assign the samples to two sets when the target bit is assumed to be zero, and then assign the sample to two sets when the target bit is assumed to be one. Comparing the differences between the two sets of each case should provide useful information. Note that the measurements collected are just the running times, not detailed traces as in power attacks.

Policies and Submission Instructions:

- This assignment must be solved **individually**. Please check the academic integrity guidelines discussed in the first lecture.
- Please submit your solution as a zip file that includes the following:
    - Your code (only .java files)
    - A report that also includes your code and observations. The report should list the speed-up that you got in the first part as a number and the results of your study in the second part as a figure. In addition, there should be a summary of your observations, conclusions and any challenges that you faced. Justify the results of your experiments.
- The name of the file must be hs_asg2_<id>.zip (replace <id> with your seat number)
- The deadline will be set by the teaching assistant. No late submissions will be accepted (unless you have a valid excuse).
- The submission form can be found through this link.