ENSIBS

PRJ 1401

RSA power analysis attack with ChipWhisperer

Cizdziel Matthieu, Richard Etienne, Moguedet Mathis

PEI-2

7 février 2024

Table des matières

1 ChipWhisperer

1.1 ChipWhisperer's purpose

ChipWhisperer is used to make power analysis attacks easy by making a confined environment that we can analyze. It also provides a lot of crypto-firmware that we can attack with some side channel attack's tutorials.

1.2 ChipWhisperer's components

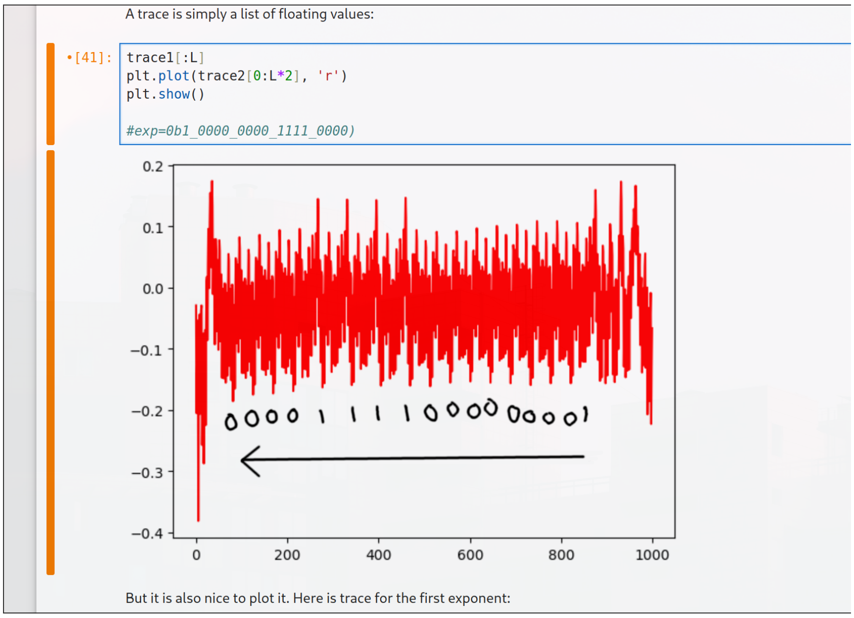
ChipWhisperer is made of 2 main components :

- a capture board used to record the current consumption and make the interface between the computer and the crypto-processor
- a target board used to plug a target chip onto.The target board is useful to quickly switch from a target chip to another one

The target chip is the place where the firmware we want to analyze is running. This chip is only running our firmware so we don't have electrical noise on the analysis. The capture board is used to send the request to the target device and receive the output of the firmware, this board also record the current consumption of the target device. By slicing the work of a computer with two boards, the ChipWhisperer tool allow us to run our firmware in a confined space.

2 First attack on RSA

For our first side channel attack on RSA we used an open source firmware and notebook found on github. This firmware use the square and multiply algorithm so the attack was based on it. Theses opensource files helped us to understand the using of simpleserial, a Chipwhisperer's library. Finally we got the following output from the capture-board.



A trace is simply a list of floating values:

```
•[41]: trace1[:L]
       plt.plot(trace2[0:L*2], 'r')
       plt.show()

       #exp=0b1_0000_0000_1111_0000)
```

But it is also nice to plot it. Here is trace for the first exponent:

FIGURE 1 – Currant consumption of the target

As we can see for every bit of the private key we can retrieve to correct value.

3 Building our own Firmware

3.1 Communication between the computer and the ChipWhisperer

To send the information from the computer to the ChipWhisperer, we use the "simpleserial.h" librairy.

4 Conclusion