Projet : attaque EMA AES-128

Thomas Prévost (CSN 2024)

Project and objectives

This project aims at identifying an AES-128 secret key used by an unknown FPGA, thanks to a study of the electromagnetic leaks of the card.

The studied data consists of 20000 measurements of 20000 clear texts and 20000 corresponding encrypted texts.

The attack

Data extraction

We begin by extracting the data from the provided files. We do this using a Ruby script, called with the following command:

```
ruby parser.rb source_folder [output_extension]
```

The raw data is then extracted and converted, then saved as separate files in the `out` folder.

First analysis & rounds identification

First of all, we need to identify the position of the various rounds in the AES algorithm.

We first plot the 4000 samples of the first available trace :

On this plot, it is possible to identify the beginning and end of the encryption.

Yet, it is not possible to identify the beginning and end of each round.

To do so, we plot the average of the 20000 traces :

We can now identify the beginning and end of each round (note that the extra first round is not an encryption round but an initiation of VHDL code).

Specifically, the last round is in the interval $[2700, 3200]$.

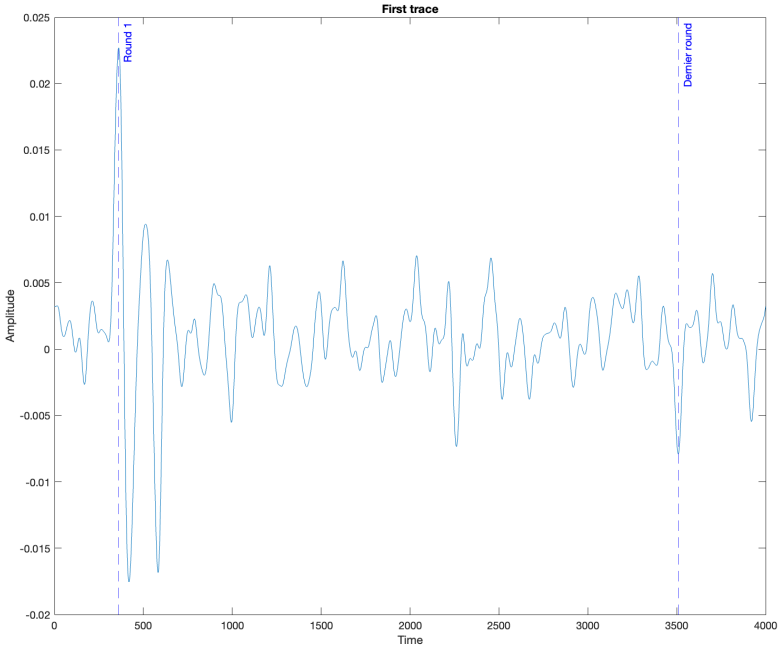

Figure 1: Analysis of first trace

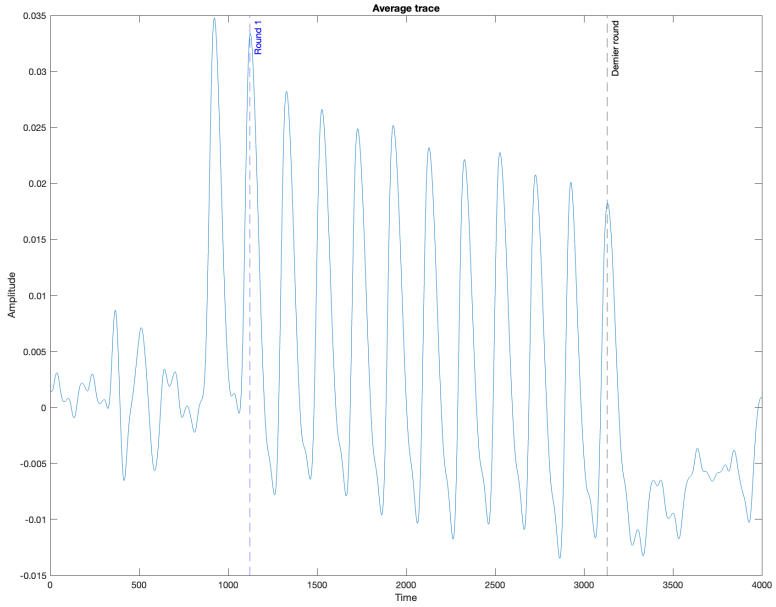

Figure 2: Rounds identification

Keys generation

Before we go further, we generate all the possible keys. These possible keys consist of 256 bits times 16 bytes, applied to each of the 20000 traces. The resulting array is then a $20000 \times 256 \times 16$ array.

Now, we will, for each possible key, apply the inverse AES algorithm :

1. `XOR(cto, key)` ;
2. inverse `shiftrow` on the previous result ;
3. inverse `subbytes` on the previous result.

Key identification

The last step is to identify the key.

To do so, we will first use the Hamming Weight method on the computed result, then correlate it with the measurements of the last round. The result is then plotted, and the key is identified.

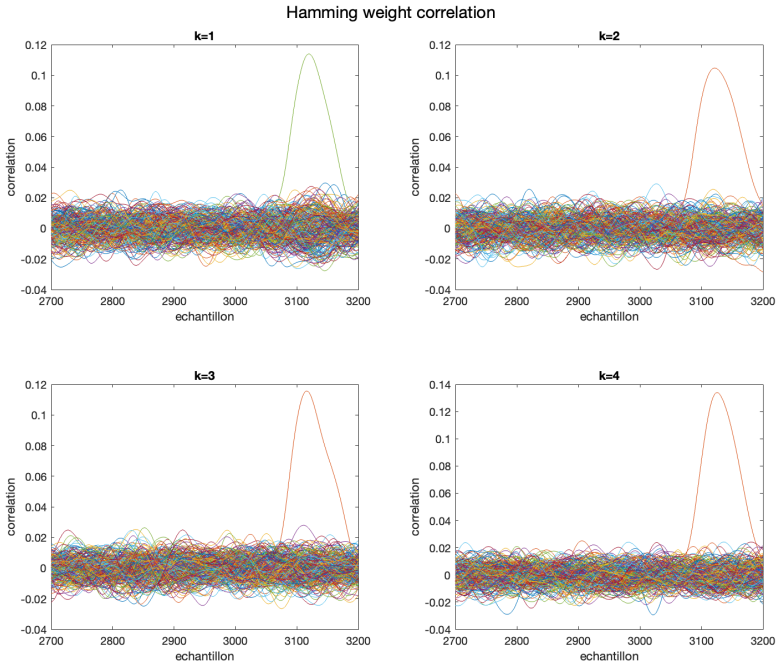

Figure 3: Identification of best candidate

We notice that the best candidate can clearly be identified.

To check the validity of the identified key, we simply calculate the theoretical result and compare it to.