Hardware Security: Side-Channel Analysis - Assignment 1

Niels van den Hork (s4572602)
Niels van Drueten (s4496604)

April 19, 2019

1 Introduction

This report discusses the second assignment of the Side-Channel Analysis of the Hardware Security course. In part 1, we have implemented the Correlation Power Analysis (CPA) against the cryptographic hardware implementation of the PRESENT cipher. In part 2, we have performed a higher-order attack against hardware using serial processing.

2 Part 1

We took the peak of the absolute Pearson correlation values per key and used this to determine which key had the largest correlation. In the following figure, the absolute correlation values is plotted per key. It is hard to see which key is the best to guess, but is between 0 and 50. The function `compute_best_key` computes the best key guess. This function computes key 15 (0b1111) as the best key guess

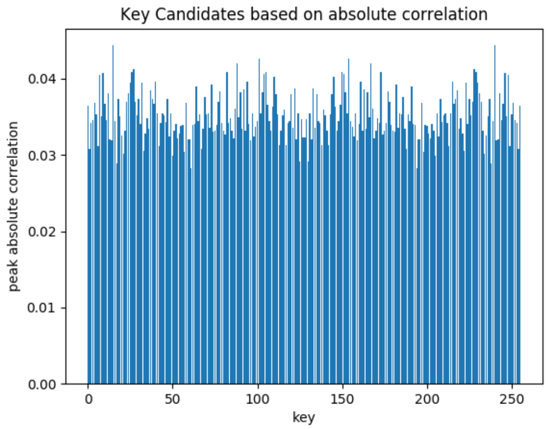
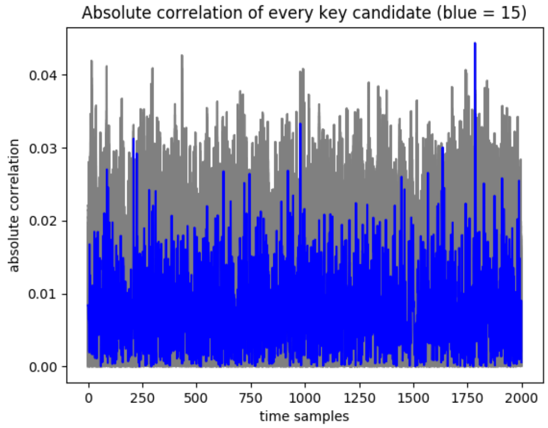
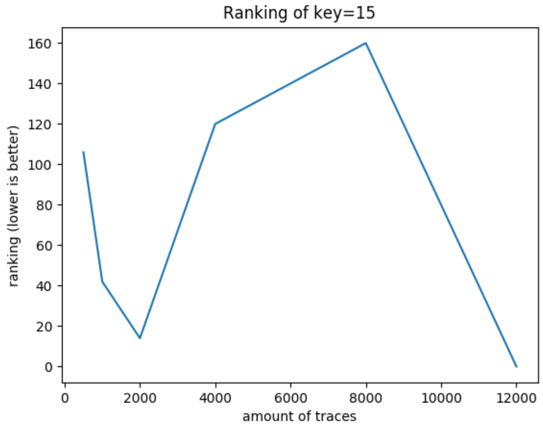


Figure 1: Caption

On the left, we have plotted the absolute Pearson correlation values for every k candidate. The top candidate (key 15) is highlighted in blue. The figure on the right shows the ranking that key 15 gets when only [500,1000,2000,4000,8000,12000] are considered.





3 Part 2

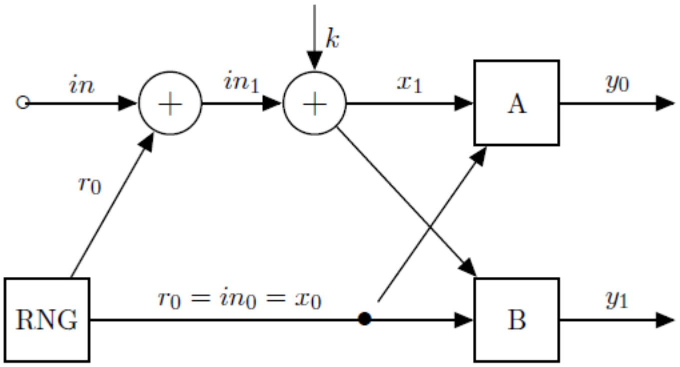


Figure 2: Caption

In this part we will extract the key that is used in traces made according to Figure 2 Where:
$A = A(x_0||x_1)$
$B = A(x_0||x_1) \oplus SBox(x_0 \oplus x_1)$

From this we can rewrite y_0 and y_1 to:
$y_0 = A(x_0||x_1)$
$y_1 = SBox(x_0 \oplus x_1) \oplus A(x_0||x_1) = SBox(in \oplus k) \oplus A(x_0||x_1)$

And we know that $y = y0 \oplus y1$ So $y = S(in \oplus k) \oplus A(x_0||x_1) \oplus A(x_0||x_1) = S(in \oplus k)$
This means that we could determine y from only in and k. And, more importantly, independently from r_0.

We can then create a value prediction matrix using by computing this y per given input for every possible key. Then we correlate these value predictions together with hardware traces. The true key (key 3) will produce the highest correlation, which we show in figure 2.

One detail is that y does not produce any 'one' value in the traces, y_0 and y_1 may occur at different timesteps in the trace. We can solve this by computing a new set for $t' = \{t_i * t_j | len(t) > j >= 0; j > i >= 0\}$ Where t is the trace. In other words, we have computed the multiplication of values for all combinations of timesteps in the trace, so we have also captured the combination where y_0 is noticeable in the first timestep and y_1 is noticeable in the second timestep. We correlate this t' against the value prediction.

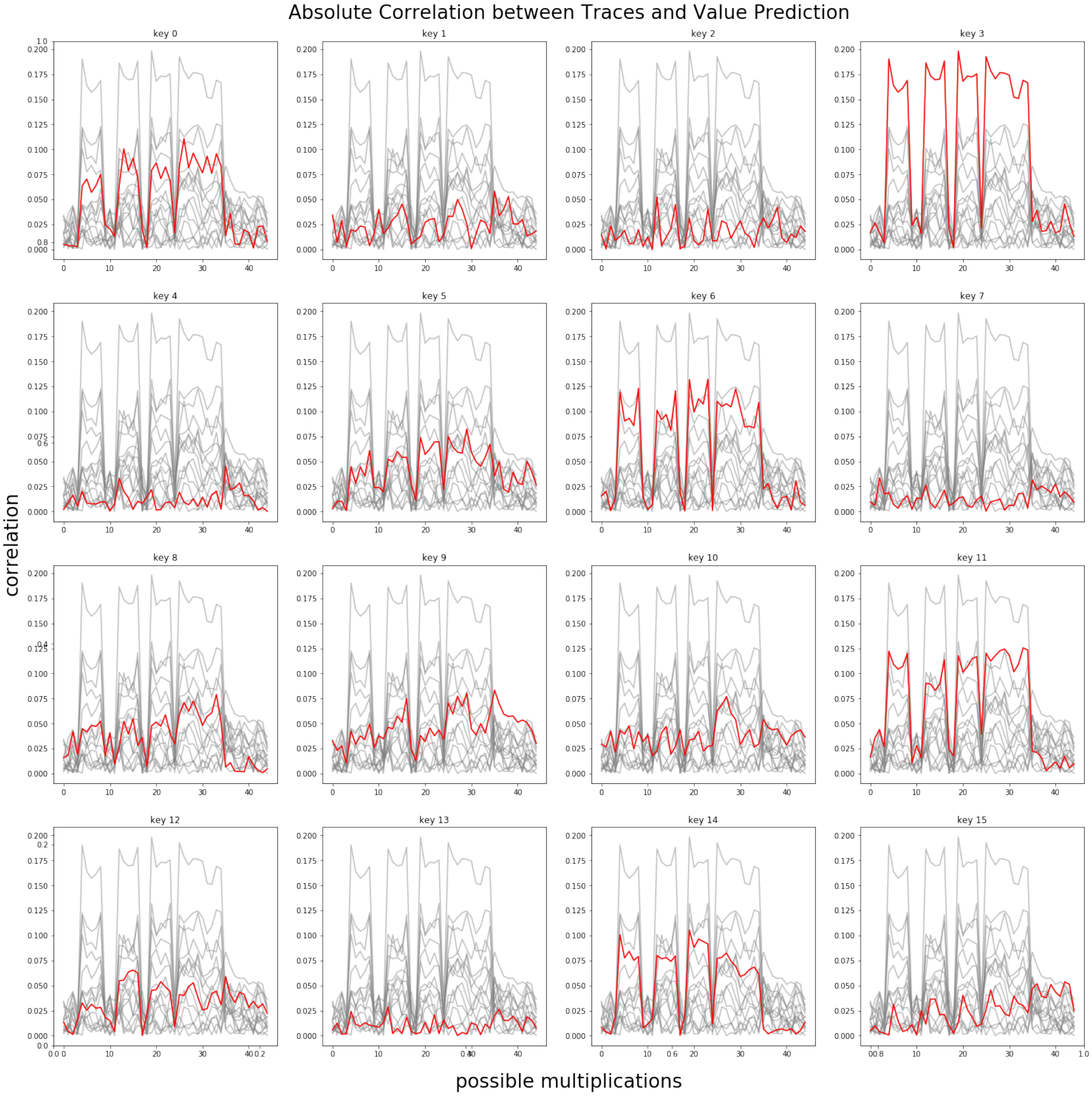


Figure 3: Absolute correlation between Traces and Value prediction per key