Timing attack against a DES implementation

Alessandro Menduni

May 6, 2015

1 Introduction

A power attack is a side channel attack, which consists in exploiting information given by the power consumed by the hardware to execute a cryptographic alghoritm. In particular, it is taken into account the dependancy between the input provided to the system and the observed power trace of the system while it was completing the operation, thus, by the use of precise measurements, an attacker can procede backwards from the output to the input. In this report it will be considered the attack against a DES hardware implementation, using as dataset a series of power traces.

2 The attack target: the LR register

The main target of the attack will be the register used in the attacked implementation for storing both sides of the results of each round, namely Ln and Rn. What this attack would exploit is the relationship between the number of bit flips occured between two rounds and the power consumed by the device; in fact, it is common knowledge that a register implemented through use of CMOS will have a power consumption directly linked to the number of state transitions that occur in a given time range.

3 Attack's working principles

The reasoning behind the attack is the following:

- Since this architecture relies on the same register to store subsequent values of L and R, it would be expected a relationship between the number of bit flips in L16 and the entity of the power trace;
- Since the attacker owns the cipertexts, she can extract L16 and combine it with her guess for the 16th round key, then walk backwards up to the value that would be assumed by L15 if K16 was correct;
- Once having obtained both L15 and L16, the attacker can compute the hamming distance of the two. This would give her an estimation of how many bits have been flipped in the register between round 15 and 16;
- Finally, the attacker tries to find the 16th round keys such that the number of bit flips, occurring in the half of the LR register between round 15 and round 16, is as correlated as possible to the amount of power consumed by the hardware to perform such operations;
- In order to make the relationship between the power traces and the number of bit flips in the register apparent, the attacker computes some kind of ranking for every guessed key, in a way that associates an higher rank to the key for which the link between the power traces and the quantity of bit flips is stronger.

A computationally feasible procedure would carry on the attack on one SBox at a time, as follows:

- It is generated every possible combination of the first 6 bits of the key
- For every key generated as such, it is computed the correlation between all the measurements and the corresponding hamming distances
- It is kept as good the key whom correlation is the highest
- Repeats for the next 6 bits of the key until all the 48 bits of 16th round key have been "guessed"

At this point the remaining bits of the 64bits key can be brute-forced by inverting the key schedule algorithm and trying all the keys over a couple plaintext-ciphertext, which is needed in order for the attack to automatically recognise whether it's been successful or not. Since this was not the case in the considered scenario, that attack should stop at the 48bits 16th round key.

4 Considerations that led to the design of the attack

The provided not working attack presented a series of architectural flaws: first of all, it was attacking 1 bit at a time, which is too unreliable since a single bit flip is a too small change in the power trace for it to be exploitable by the attacker and this flaw was made evident by the fact that attacking different bits of the same SBox led to different guesses for the same SBox; moreover, it was not isolating the transitions 1-¿0 and 0-¿1 but it was just considering all the cases that could lead to either 1 or 0 (including cases such as 1-¿1 and 0-¿0), such thing is imprecise and based on the wrong assumption that a CMOS has an higher consumption when it's in the 1-state than when it's in the 0-state; finally, that attack considered the whole trace for its statistical analysis, but it should be better to trim them in order to have data regarding the last round only. It is in fact possible to identify the part of the trace regarding the interesting rounds by looking at the plot of the traces and knowing the tool used to measure the signal: indeed, every 25 points on the traces there's one clock stroke and it can be spotted the beginning and the end of the 16 DES rounds from point 200 to point 600 in the x-axis. Considering what has been discussed so far, the final attack proposed in this report has the following features: it attacks 6 bits of the 16th round key at a time; it builds an hamming distance attack, thus considering all the bit flips occurring in the register which thing is more distinctly highlighted in the power traces; it analyses only the part of the power trace corresponding to the clock period of the 16th round of the DES.

5 The ranking system

The selected method relies on the Pearson product-moment correlation coefficient to measure the desired correlation; this strategy takes into account all the chipertexts in the data set and it is much more stable. Such PCC coefficient is computed by considering as X variable the power traces, whereas the Y variable contains the hamming distances between L15 and L16.

6 Results and environment

The machine used to run the experiments is a laptop ASUS K550JK mounting an i7-4710HQ with 4GB of RAM DDR3L-1600. The data file used to test the solution is the one provided and the recovred key is f0be2e5b242c with a stable minimum of 228 experiments needed.