VET : Side Channel Attacks

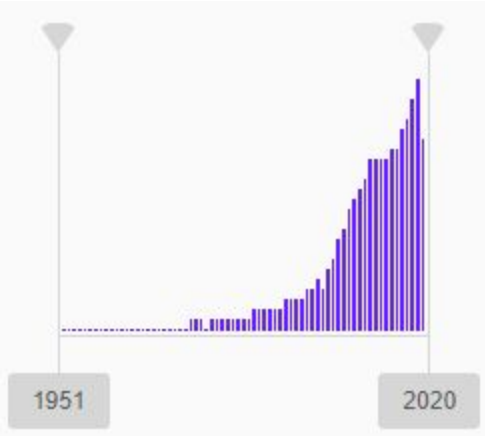
Abstract of *"DES and Differential Power Analysis"*

Dorian BESCON

M2 Cybersécurité

Actual and Historical State

If we look at the number of publications concerning side channel attacks, we can see that their number is clearly on the rise (figure on the right), especially since the 1998 publication of Paul Kocher, Joshua Jaffe and Benjamin Jun describing DPA-type attacks for the first time.



This paper was released in 1999, shortly after the previously mentioned publication, when DPA attacks were just discovered.

Publication contribution

This publication provides DES and RSA implementations that are resistant to subchannel attacks, which was a good alternative to other countermeasures against this kind of side-channel attacks.

Abstract

Types of attacks

This publication begins by explaining in detail how side channel attacks work. It's describing how **DPA** attacks differ from **SPA** attacks :

SPA consists of measuring the power consumed by an electronic circuit in order to deduce the operations carried out. Each instruction carried out by a microprocessor uses a certain number of transistors. Of course, the power consumed is very low, its variations are subtle and extremely fast. Nevertheless, the measuring instruments in use today allow extremely fine measurements, with resolutions of less than micro amperes and sampling frequencies up to gigahertz.

DPA attacks appeared in 1998, following the publication of Paul Kocher, Joshua Jaffe, and Benjamin Jun on Differential Consumption Analysis. The idea they explore is the combination of consumption frame analysis with statistical methods covering thousands of operations. The key presented to the cryptographic algorithm will always trigger a different behavior depending on whether it is false or exact, the current

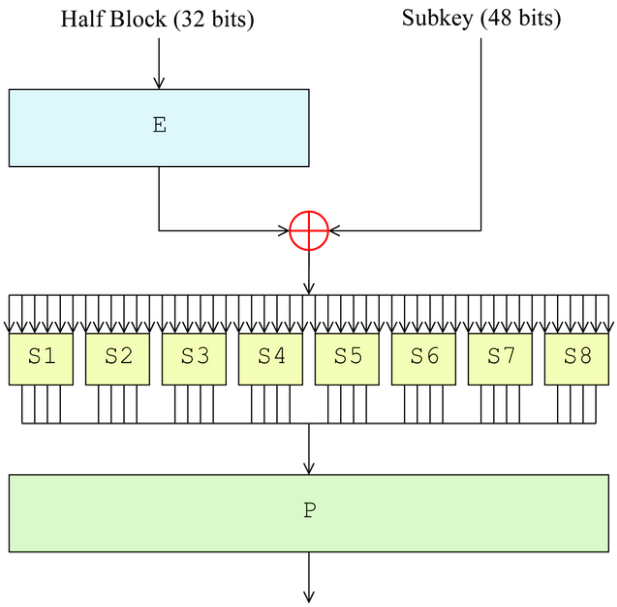
consumption, measured over a large number of samples, will always be a clue to the secret key.

The publication of Louis Goubin and Jacques Patarin is only focusing on the second type described above : DPA. They make a precise description of how it works :

The DPA attacks assume that the attacker can have many informations during the execution of the computation, such as the power consumption of the processor or the electromagnetic radiations of the circuit.

The goal of the attack is to get information about the secret key. To achieve that, an attacker will use consumption records for a lot of computations that have been using the same secret key.

The **example** taken in the publication is the attack of the DES algorithm (which was one of the most popular symmetric-key algorithms in 1999, just before it was declared obsolete). Here are the steps described for the DPA attack :



1. We measure the consumption of the first round for 1000 DES computations. We denote by E_1, …, E_{1000} the input values for those 1000 computations and C_1, …, C_{1000} the electric consumption curves. MC is the mean of those curves.
2. We focus on the first output bit of the first S-box during the first round (*b*). This value depends on only 6 bits of the secret key (*clearly visible in the figure on the right, that describes DES*). The attacker can now make an hypothesis on those involved 6 bits. He computes the expected values of b and splits the E (input values) into **2 groups** : Those giving *b* = 0 and those giving *b* = 1.
3. We can now compute the mean MC' for the inputs. If there is a big difference between MC and MC' (*figures 1 and 2 in* annexes), we can deduce that the 6 bits

associated with MC' are correct. If MC and MC' are not very different, we repeat step 2 with different 6 bits.

4. We repeat steps 2 and 3 targeting bit b in the second S-box, then the third etc … We now have 48 bits of the secret key.

5. The last bits can be found by exhaustive search.

Counter measures

It is very difficult to protect oneself from such an attack. Some countermeasures do exist, but they are often restrictive and unrealistic in a production context. They include the following :

- The **reduction of the consumed power**, making the variations imperceptible. Nevertheless, as the performance of the measuring devices is only increasing, an attacker with a large number of samples could achieve his goal.
- **Electromagnetic shielding**, avoiding the measurement itself. However, this is very expensive.
- Drowning the signal in **noise**, even temporally, making the attack so complex and requiring so many samples that it becomes impossible.

Securing algorithms

The methods described above are mostly hardware targeted methods. In this paper, the authors describe a method to protect against DPA based on a new implementation of the encryption algorithm itself.

DES for DPA resistance

The method consists in avoiding storing intermediate values V (S-box inputs) directly in memory. We therefore divide this variable V into 2 variables V1 and V2 such that V = V1 ⊕ V2 and therefore V' = V'1 ⊕ V'2. (Annexes 3 and 4)

The disadvantage of this implementation is the amount of available memory required. The size required is 32 Kbytes which was too much for devices like smartcards in 1999 : We need 2 times more S-Boxes than with the original algorithm.

The modified algorithm also makes usage of a secret function *A* that is reducing 12 bits into 4 bits. This function will be used in the new S-boxes that now computes the output bits this way :

$$(v'_1, v'_2) = S'(v_1, v_2) = (A(v_1, v_2), S(v_1 \oplus v_2) \oplus A(v_1, v_2)).$$

To solve the problem of devices with a small amount of available memory, the authors offer to use the same A function described above in the 8 initial s-boxes of DES so that we have only 9 new S-boxes instead of 16 (18 Kbytes instead of 32).

Annexes

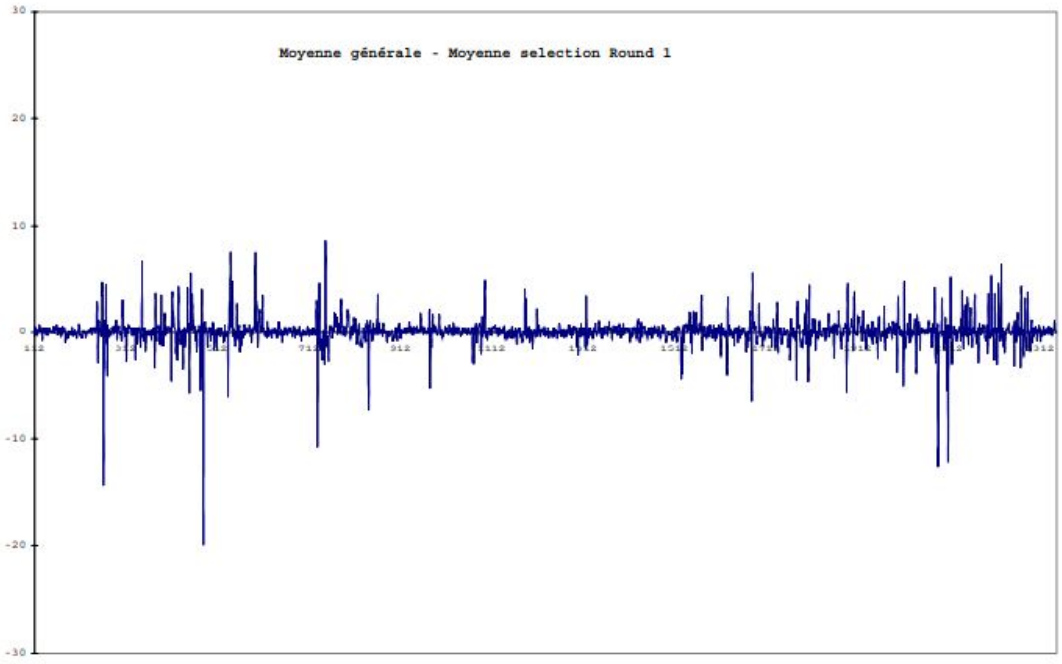


Figure 1 : MC' with **incorrect** 6 bits

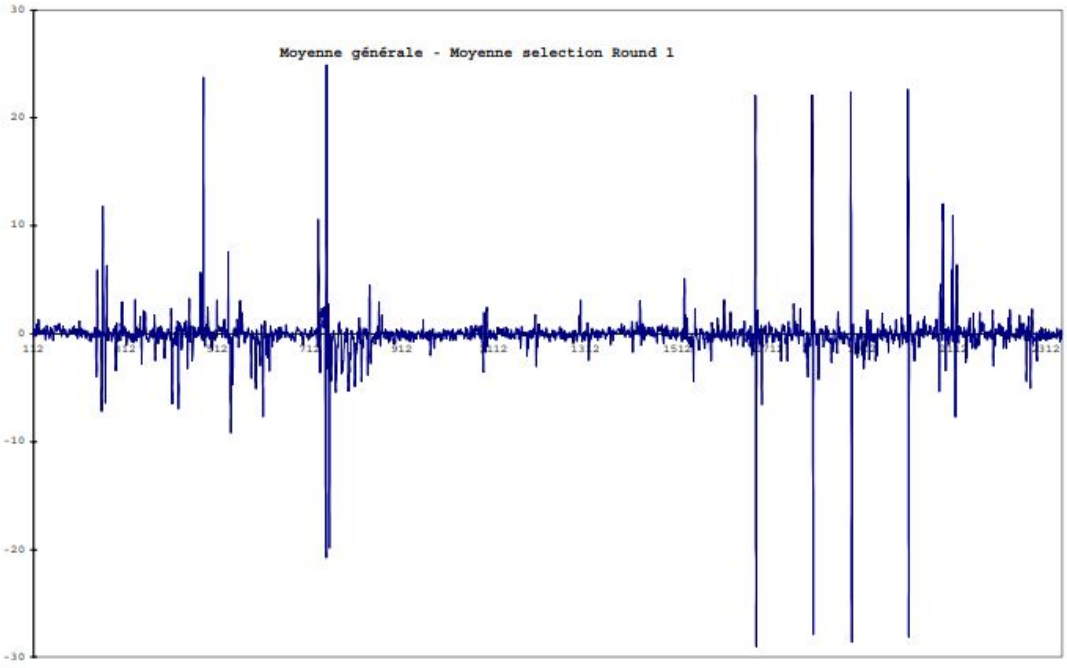


Figure 2 : MC' with **correct** 6 bits

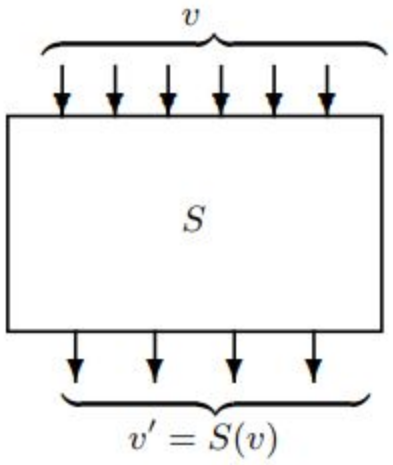
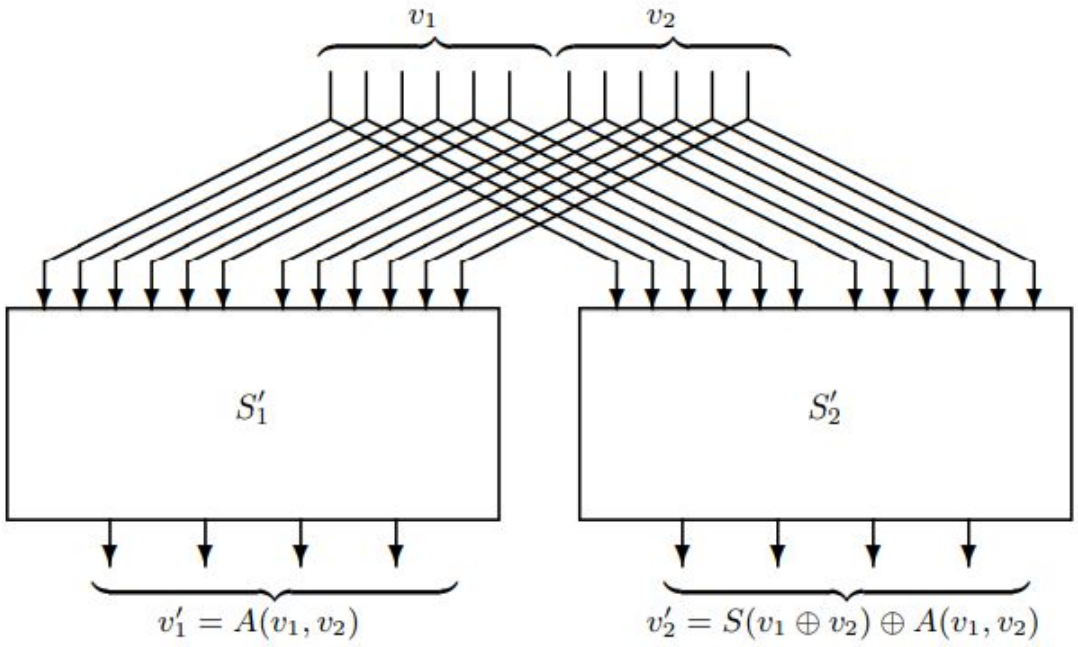


Figure 3 : V appears in RAM



Modified implementation: the values $v = v_1 \oplus v_2$ and $v' = v'_1 \oplus v'_2$ never explicitely appear in RAM

Figure 4 : V and V' doesn't appears in ram (**Modified implementation**)

Sources

[1] “Power Analysis” Wikipedia. [Online]. Available : Power Analysis

[2] “DES and Differential Power Analysis - The duplication method” Louis Goudin, Jacques Patarin. *1999*.

[3] “Actual and Historical State of Side Channel Attacks Theory” Andrey V. Krasovsky, Ekaterina A. Maro. *2019*.