

$$y' = S'[x + m_1] = y + m_2 = S[x] + m_2$$

where m_2 is a corresponding random mask which masks the output value of the substitution table. At the end of the algorithm, the result is unmasked to obtain the final result (the original data, encrypted and unmasked).

Nevertheless, attacks will sometimes successfully overcome the difficulties introduced by prior art masking. In particular, some types of attacks such as HO-DPA (High Order Differential Power Analysis) attacks can be especially difficult to avoid under certain circumstances. This is explained in particular in the article "On Second-Order Differential Power Analysis" by Marc Joye, Pascal Paillier and Berry Schoenmakers, published in Cryptographic Hardware and Embedded Systems, CHES 2005, Lecture Notes in Computer Science 3659 (2005), 293-308, Springer Verlag. Therefore, when an attacker successfully correlates power consumption (or other information of this type) with calculations multiple times, he can sometimes overcome the masking.

The invention improves this situation.

According to a first aspect of the invention, ~~The invention relates to a~~ method for securing the execution of a cryptographic algorithm against passive sniffing is disclosed, said method carrying out a masking of data processed by the cryptographic algorithm. The masking of said data includes a transformation step of the type $x' = x.L + c$, where x is data to be masked (such as input data to the cryptographic algorithm, intermediate sensitive data, or a key), x' is the corresponding masked data, c is a codeword included in a linear code C , and L is a matrix consisting of linearly independent vectors not included in the linear code C . The method may consist of a modified implementation of the algorithm, for example modified into a functionally equivalent algorithm (meaning it produces the same output for the same input) which includes at least one step of masking by transformation (such as linear encoding), and at least one corresponding step

while keeping the same one makes it possible to maintain an acceptable speed particularly for devices which have limited resources, such as entry-level smart cards having a very slow processor and not much memory.

5 In the two previous embodiments, it can be arranged to determine a nonlinear operation S' such that $c' = c$, which simplifies the unmasking operation. It is in any event necessary to unmask what was masked, so that the secure cryptographic algorithm can produce the same result as the cryptographic algorithm without the added security.

10 According to a second aspect of the invention, The invention also relates to an electronic device is disclosed, the electronic device including a unit for executing the cryptographic algorithm (the cryptographic algorithm execution unit) as well as an associated masking module. The masking module is configured to apply a transformation of the type $x' = x.L + c$, where x is data to be masked, x' is the corresponding masked data, c is a codeword included in a linear code C , and L is a matrix consisting of linearly independent vectors not included in the linear code C .

20 The embodiments described above with respect to the method can be transposed to the device; in particular, according to one embodiment, the masking module is arranged to choose a codeword c randomly during each execution of the cryptographic algorithm. According to one embodiment, the masking module chooses the matrix L randomly one time only for all executions of the cryptographic algorithm. According to one embodiment, the masking module is arranged to perform the masking before the cryptographic algorithm is applied, and to perform an unmasking operation after the cryptographic algorithm is applied. According to one embodiment, the cryptographic algorithm of the execution unit is an algorithm implementing a nonlinear operation S , and the masking module is arranged to replace the nonlinear operation S with a nonlinear operation S' such that $S'(x.L + c) = S(x).L + c'$, where c' is a codeword of the linear code C . According to one embodiment, the cryptographic algorithm of the execution unit includes