

CLAIMS

1. A cryptography circuit (21) comprising a functional key k_c for executing a cryptography algorithm, characterized in that said circuit comprises a second key k_i independent of k_c and specific to each instance of said circuit, making it possible to protect the latter against the attacks exploiting the side channels of said circuit.
- ~~2. The circuit as claimed in claim 1, characterized in that the functional key k_c being is masked by the second key k_i by combining the two keys via the XOR operation, an input variable x being encrypted by the masked key $k_c \oplus k_i$.~~
- the second key k_i being created by a Physically Unclonable Function Physically Obfuscated Key.
23. The circuit as claimed in claim 1, characterized in that the second key k_i serves to protect the key by virtue of a confidential implementation.
34. The circuit as claimed in claim 1, characterized in that the second key k_i serves to protect a confidential algorithm.
45. The circuit as claimed in claim 34, characterized in that the confidential algorithm comprises a standard cryptographic algorithm customized by the bracketing of two secret functions (30, 31) protected by masking with the key k_i .
- ~~6. The circuit as claimed in any one of the preceding claims, characterized in that the second key k_i is created by a function of the PUF (Physically Unclonable Function) or POK (Physically Obfuscated Key) type.~~

57. The circuit as claimed in any one of claims 1 to 45, characterized in that the second key k_i is programmed after fabrication of said circuit, by customization with a unique random value in a secure enclosure.
- 5 68. The circuit as claimed in any one of the preceding claims, characterized in that the masking introduced by the second key k_i is protected against HO-DPA high-order attacks.
79. The circuit as claimed in any one of the preceding claims, characterized
10 in that the knowledge of the second key k_i , serving as implementation key unique to a circuit, allows the use of a protection control procedure to privileged users responsible for said control.
840. The circuit as claimed in any one of the preceding claims, characterized
15 in that it is realized on a programmable circuit of the FPGA type.
944. The circuit as claimed in any one of the preceding claims, characterized in that the second key k_i may be customized by way of an FPGA's programming file.
- 20 1042. The circuit as claimed in any one of claims 1 to 79, characterized in that it is realized by a software implementation.
1143. The circuit as claimed in any one of claims 940 or 1044, characterized in
25 that it comprises a third key k_b for encrypting the programming file (25) of said FPGA circuit, this conferring the confidentiality of the external storage and of the transfer of the key k_i to the FPGA.
1244. The circuit as claimed in any one of the preceding claims, characterized
30 in that the cardinal of the second key k_i is equal to the cardinal of the functional key k_c .

1315. The circuit as claimed in any one of claims ~~1113~~ or ~~1214~~, characterized in that the cardinal of the third key k_b is greater than or equal to the cardinal of the functional key k_c .
- 5
1416. The circuit as claimed in any one of the preceding claims, characterized in that the encryption algorithm is the DES algorithm.