ABSTRACT

CRYPTOGRAPHY CIRCUIT PARTICULARLY PROTECTED AGAINST INFORMATION-LEAK OBSERVATION ATTACKS BY THE CIPHERING THEREOF

The present invention relates to a cryptography circuit, protected notably against information-leak observation attacks.

The cryptography circuit (21) comprises a functional key k_c for executing a cryptography algorithm. It comprises a second key k_i unique and specific to the circuit making it possible to protect by masking the functional and confidential key k_c or a confidential implementation of the algorithm.

Figure 4