

ABSTRACT

CRYPTOGRAPHY CIRCUIT PROTECTED AGAINST OBSERVATION
ATTACKS, IN PARTICULAR OF A HIGH ORDER

The present invention relates to a cryptography circuit protected against observation attacks.

The cryptography circuit comprises at least one register R (22) providing a variable x masked by the mask m , the masked variable being encrypted by
5 a first substitution box S (1) in a cyclic manner. The circuit also comprises a mask register M (23) delivering at each cycle a mask m_i , the transformation of m , the mask m being extracted from m_i before being encrypted by a
second substitution box S' (21), the new mask m' obtained on output from this box S' (21) is transformed into a mask m'_i before being stored in the
10 mask register M(23)

The transformation consists of a bijection or a composition law making it possible to reduce or indeed to cancel any high-order attack in accordance with a model of activity of the registers R and M.

The invention applies notably for the protection of cryptography circuits
15 against high-order observation attacks on installations based on masking.

Figure 6



162162



G00002