ABSTRACT

METHOD FOR PROTECTING A PROGRAMMABLE CRYPTOGRAPHY CIRCUIT, AND CIRCUIT PROTECTED BY SAID METHOD

The present invention relates to a method for protecting a programmable cryptography circuit and to a circuit protected by such a method.

The circuit is composed of memory-based cells defining the logic function of each cell, integrating a differential network capable of carrying out calculations on pairs of binary variables, comprising a first network of cells implementing logic functions on the first component of the pairs and a second network of dual cells operating in complementary logic on the second component of the pair. A calculation step comprises at least one precharge phase (41), in which the variables are put into a known state at the output of the cells, followed by an evaluation phase (43) in which a calculation is made by the cells.

A phase (42, 44) of synchonizing the variables is inserted before the evaluation phase or the precharge phase in each cell capable of receiving several signals conveying input variables, the synchronization being carried out on the most delayed signal.

The invention applies notably for protecting this type of circuit against differential power analysis attacks.

Figure 4.