

ABSTRACT**METHOD FOR PROTECTING THE DECRYPTING OF THE
CONFIGURATION FILES FOR PROGRAMMABLE LOGIC CIRCUITS AND
CIRCUIT IMPLEMENTING THE METHOD**

The subject of the invention is a method for protecting a programmable logic circuit (100, 200), characterized in that the data file(s) used for the configuration of the programmable resources of the circuit are stored in a non-volatile memory (107, 207) after having been encrypted (112), a decryption module internal to the circuit (103, 203) being responsible for decrypting the file(s) by using a secret key (102, 202) stored in the circuit, the decryption module being protected against attacks aiming to obtain the key during the decryption operation by implementing at least one countermeasure technique.

Another subject of the invention is a programmable logic circuit of FPGA type protected against observation and/or fault-injection attacks during the decryption operation by using the method according to one of the preceding claims.

Figure 2

