Title (en)

METHOD OF PROTECTING CONFIGURATION FILES FOR PROGRAMMABLE LOGIC CIRCUITS FROM DECRYPTION AND CIRCUIT IMPLEMENTING THE METHOD

Title (de)

VERFAHREN ZUM SCHUTZ VON KONFIGURATIONSDATEIEN FÜR PROGRAMMIERBARE LOGIKSCHALTKREISE AUS ENTSCHLÜSSELUNGEN SOWIE SCHALTKREIS ZUR ANWENDUNG DIESES VERFAHRENS

Title (fr)

PROCÉDÉ DE PROTECTION DU DÉCRYPTAGE DES FICHIERS DE CONFIGURATION DE CIRCUITS LOGIQUES PROGRAMMABLES ET CIRCUIT METTANT EN OEUVRE LE PROCÉDÉ

Publication

EP 2316096 A1 20110504 (FR)

Application

EP 09806409 A 20090730

Priority

- EP 2009059891 W 20090730
- FR 0855536 A 20080812

Abstract (en)

[origin: WO2010018072A1] The subject of the invention is a method for protecting a programmable logic circuit (100, 200) characterized in that the data file or files used for configuring 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 in charge of decrypting the file or files using a secret key (102, 202) stored in the circuit, the decryption module being protected against attacks aimed at obtaining the key during the decryption operation by deploying at least one counter-measure technique. The subject of the invention is also a programmable logic circuit of FPGA type protected against attacks by observation and/or injection of faults during the decryption operation using the method according to one of the preceding claims.

IPC 8 full level

G06F 21/75 (2013.01); **G06F 21/76** (2013.01)

CPC (source: EP KR US)

G06F 21/602 (2013.01 - KR); **G06F 21/75** (2013.01 - KR); **G06F 21/755** (2017.07 - EP US); **G06F 21/76** (2013.01 - EP KR US)

Citation (search report)

See references of WO 2010018072A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

WO 2010018072 A1 20100218; CA 2733546 A1 20100218; CN 102119390 A 20110706; EP 2316096 A1 20110504; FR 2935078 A1 20100219; FR 2935078 B1 20121116; JP 2012505442 A 20120301; KR 20110083592 A 20110720; US 2011258459 A1 20111020

DOCDB simple family (application)

EP 2009059891 W 20090730; CA 2733546 A 20090730; CN 200980131328 A 20090730; EP 09806409 A 20090730; FR 0855536 A 20080812; JP 2011522469 A 20090730; KR 20117003338 A 20090730; US 200913058548 A 20090730