Title (en)

DEVICE FORMING A LOGIC GATE FOR MINIMIZING THE DIFFERENCES IN ELECTRICAL OR ELECTROMAGNETIC BEHAVIOR IN AN INTEGRATED CIRCUIT MANIPULATING A SECRET

Title (de)

EINRICHTUNG ZUR BILDUNG EINES LOGIKGATTERS ZUR MINIMIERUNG DER UNTERSCHIEDE BEIM ELEKTRISCHEN ODER ELEKTROMAGNETISCHEN VERHALTEN IN EINER EIN GEHEIMNIS MANIPULIERENDEN INTEGRIERTEN SCHALTUNG

Title (fr)

DISPOSITIF FORMANT PORTE LOGIQUE ADAPTEE POUR MINIMISER LES DIFFERENCES DE COMPORTEMENT ELECTRIQUE OU ELECTROMAGNETIQUE DANS UN CIRCUIT INTEGRE MANIPULANT UN SECRET

Publication

EP 1878115 A1 20080116 (FR)

Application

EP 06754998 A 20060504

Priority

- EP 2006062037 W 20060504
- FR 0504569 A 20050504

Abstract (en)

[origin: WO2006117391A1] The invention relates to a logic gate whose consumption is independent from its input data and its logic state. To this end, the device uses logic means forming switches (220, 720, 750). The interest in having a device of this type is, for example, to protect chip cards and other cryptosystems from attacks via auxiliary channels such as collision attacks by and attacks by differential analysis of current, power or consumption. This protection is provided by the hardware. The invention is for integration in all devices requiring such a protection.

IPC 8 full level

H03K 19/173 (2006.01)

CPC (source: EP US)

G06F 21/755 (2017.07 - EP US); **H03K 19/1731** (2013.01 - EP US)

Citation (search report)

See references of WO 2006117391A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 2006117391 A1 20061109; CA 2607553 A1 20061109; EP 1878115 A1 20080116; FR 2885461 A1 20061110; FR 2885461 B1 20070727; US 2009302882 A1 20091210; US 7863926 B2 20110104

DOCDB simple family (application)

EP 2006062037 W 20060504; CA 2607553 A 20060504; EP 06754998 A 20060504; FR 0504569 A 20050504; US 91977306 A 20060504