Title (en)

METHOD FOR COUNTERMEASURING IN AN ELECTRONIC COMPONENT

Title (de)

GEGENMASSNAHMENVERFAHREN IN EINEM ELEKTRONISCHEN BAUELEMENT

Title (fr)

PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE

Publication

EP 1639450 A1 20060329 (FR)

Application

EP 04741817 A 20040617

Priority

- EP 2004051142 W 20040617
- FR 0307380 A 20030618

Abstract (en)

[origin: WO2004111833A1] The invention relates to a method for countermeasuring in an electronic component while using a public key cryptographic algorithm. The invention involves the use of a public key cryptographic algorithm containing an exponentiation calculation y=g &cir& d, in which g and y are elements of specified group G noted in a multiplicative manner and d is a predetermined number.

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/723 (2013.01 - EP US); **G06F 7/725** (2013.01 - EP US); **H04L 9/002** (2013.01 - EP US); **H04L 9/3013** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); H04L 2209/04 (2013.01 - EP US); H04L 2209/12 (2013.01 - EP US)

Citation (search report)

See references of WO 2004111833A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

FR 2856538 A1 20041224; **FR 2856538 B1 20050812**; EP 1639450 A1 20060329; US 2007121935 A1 20070531; WO 2004111833 A1 20041223

DOCDB simple family (application)

FR 0307380 A 20030618; EP 04741817 A 20040617; EP 2004051142 W 20040617; US 56127604 A 20040617