Title (en)

METHOD FOR COUNTERMEASURING BY MASKING THE ACCUMULATOR IN AN ELECTRONIC COMPONENT WHILE USING A PUBLIC KEY CRYPTOGRAPHIC ALGORITHM

Title (de)

VERFAHREN FÜR GEGENMASSNAHMEN DURCH MASKIERUNG DES AKKUMULATORS IN EINER ELEKTRONSICHEN KOMPONENTE BEI GLEICHZEITIGER BENUTZUNG EINES KRYPTOGRAPHISCHEN ALGORITHMUS MIT ÖFFENTLICHEM SCHLÜSSEL

Title (fr)

PROCÉDÉ DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR

Publication

EP 1639451 A2 20060329 (FR)

Application

EP 04766054 A 20040617

Priority

- EP 2004051144 W 20040617
- FR 0307379 A 20030618

Abstract (en)

[origin: WO2004111831A2] The invention relates to a method for countermeasuring in an electronic component while using a public key cryptographic algorithm. The invention is characterized in that the method comprises an exponentiation calculation with a left-to-right exponentiation algorithm y=g &cir& d, in which g and y are elements of the specified group G noted in a multiplicative manner and d is a predetermined number. The inventive method is also characterized by comprising a random selection step at the beginning of or during the execution of said exponentiation algorithm in a deterministic or probabilistic manner for masking the accumulator A.

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); G06F 2207/7228 (2013.01 - EP US); G06F 2207/7247 (2013.01 - EP US); G06F 2207/7285 (2013.01 - EP US)

Citation (search report)

See references of WO 2004111831A2

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 2856537 A1 20041224; **FR 2856537 B1 20051104**; EP 1639451 A2 20060329; US 2006282491 A1 20061214; WO 2004111831 A2 20041223; WO 2004111831 A3 20051222

DOCDB simple family (application)

FR 0307379 A 20030618; EP 04766054 A 20040617; EP 2004051144 W 20040617; US 56123404 A 20040617