Title (en)

CRYPTOGRAPHIC METHOD COMPRISING A MODULAR EXPONENTIATION SECURED AGAINST HIDDEN-CHANNEL ATTACKS, CRYPTOPROCESSOR FOR IMPLEMENTING THE METHOD AND ASSOCIATED CHIP CARD

Title (de)

KRYPTOGRAFISCHES VERFAHREN MIT EINER MODULAREN POTENZIERUNG, DIE GEGEN VERBORGENE KANALANGRIFFE GESCHÜTZT IST, SOWIE KRYPTOPROZESSOR ZUR UMSETZUNG DES VERFAHREN UND ZUGEHÖRIGE CHIP-KARTE

Title (fr)

PROCÉDÉ CRYPTOGRAPHIQUE COMPRENANT UNE EXPONENTIATION MODULAIRE SÉCURISÉE CONTRE LES ATTAQUES À CANAUX CACHÉS, CRYPTOPROCESSEUR POUR LA MISE EN OEUVRE DU PROCÉDÉ ET CARTE À PUCE ASSOCIÉE

Publication

EP 1969459 A1 20080917 (FR)

Application

EP 06841618 A 20061222

Priority

- EP 2006070206 W 20061222
- FR 0513305 A 20051226

Abstract (en)

[origin: FR2895609A1] The method involves masking an operand e.g. message to be encrypted, with a random number by multiplying the operand with a parameter including a constant and exponent. A modular exponentiation of the operand masked by an exponent e.g. public or private key, is formed by using a Montgomery multiplier. An exponentiation result e.g. signed message, is unmasked by removing the random number from the exponentiation result. Independent claims are also included for the following: (1) a cryptoprocessor for implementing a cryptographic method (2) a smart card comprising a cryptoprocessor.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/723 (2013.01 - EP US); **H04L 9/002** (2013.01 - EP US); G06F 7/728 (2013.01 - EP US); G06F 2207/7238 (2013.01 - EP US); G06F 2207/7257 (2013.01 - EP US); H04L 2209/046 (2013.01 - EP US)

Citation (search report)

See references of WO 2007074149A1

Citation (examination)

WO 2005048008 A2 20050526 - MILSYS LTD [IL], et al

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)

FR 2895609 A1 20070629; CN 101346691 A 20090114; EP 1969459 A1 20080917; US 2010014656 A1 20100121; US 8265266 B2 20120911; WO 2007074149 A1 20070705

DOCDB simple family (application)

FR 0513305 A 20051226; CN 200680049130 A 20061222; EP 06841618 A 20061222; EP 2006070206 W 20061222; US 8661906 A 20061222