Title (en)

SECURE METHOD FOR PERFORMING A MODULAR EXPONENTIATION OPERATION

Title (de)

GESICHERTES VERFAHREN ZUM REALISIEREN EINER MODULAREN POTENTIERUNGSOPERATION

Title (fr)

PROCEDE SECURISE DE REALISATION D'UNE OPERATION D'EXPONENTIATION MODULAIRE

Publication

EP 1419434 A1 20040519 (FR)

Application

EP 02772476 A 20020731

Priority

- FR 0202771 W 20020731
- FR 0110671 A 20010810

Abstract (en)

[origin: FR2828608A1] The encryption process produces an exponential operation of the type U=VW modulo X where U,V and W are whole numbers. W is formed as a masked parameter chosen randomly each execution period. The masking parameter is a fractional 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); **H04L 9/002** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); G06F 2207/7242 (2013.01 - EP US); G06F 2207/7257 (2013.01 - EP US); H04L 2209/04 (2013.01 - EP US)

Citation (search report)

See references of WO 03014916A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

FR 2828608 A1 20030214; **FR 2828608 B1 20040305**; CN 1568457 A 20050119; EP 1419434 A1 20040519; US 2004184604 A1 20040923; WO 03014916 A1 20030220

DOCDB simple family (application)

FR 0110671 A 20010810; CN 02820000 A 20020731; EP 02772476 A 20020731; FR 0202771 W 20020731; US 48634004 A 20040430