Title (en)

METHOD FOR ACCELERATING CALCULATIONS IN MODULAR ARITHMETIC

Title (de)

KRYPTOGRAPISCHE BERECHNUNG NACH DEM MOMTGOMERY-VERFAHREN

Title (fr)

CALCUL CRYPTOGRAPHIQUE SUIVANT LA METHODE DE MONTGOMERY

Publication

EP 1532519 A2 20050525 (FR)

Application

EP 03755658 A 20030729

Priority

- FR 0350022 W 20030729
- FR 0209942 A 20020805

Abstract (en)

[origin: FR2843211A1] Method has the following steps: use of a first algorithm for replacing an argument stored in 2q words by a result which is congruent to modulo N of the said argument and of which the q words of low weighting are zero; and use of a first operator for taking two entries each stored in q words and outputting a number W also stored in q words, of which the product multiplied by R is congruent modulo N with the product of the two inputs. R is a power of 2, greater than N.

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP)

G06F 7/728 (2013.01)

Citation (search report)

See references of WO 2004015559A2

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 PT RO SE SI SK TR

DOCDB simple family (publication)

FR 2843211 A1 20040206; **FR 2843211 B1 20050520**; AU 2003273500 A1 20040225; CA 2494769 A1 20040219; EP 1532519 A2 20050525; WO 2004015559 A2 20040219; WO 2004015559 A3 20040513

DOCDB simple family (application)

FR 0209942 A 20020805; AU 2003273500 A 20030729; CA 2494769 A 20030729; EP 03755658 A 20030729; FR 0350022 W 20030729