Title (en)

MULTIPLICATION IN A FINITE FIELD

Title (de)

MULTIPLIKATION IN EINEM ENDLICHEN FELD

Title (fr)

MULTIPLICATION DANS UN CHAMP FINI

Publication

EP 1636932 A2 20060322 (EN)

Application

EP 04735781 A 20040602

Priority

- IB 2004050827 W 20040602
- EP 03101735 A 20030613
- EP 04735781 A 20040602

Abstract (en)

[origin: WO2004112307A2] An apparatus for performing a multiplication in a finite field Fq ={O, 1, alpha, (alpha<2>,..., alpha<q-2> , or, in an index representation, Fq = {x0, x1,..., xq-1 } where each element xj of the field is represented by a respective index j indicated as j=i(xj). A memory 410 includes a logarithm table L 416 with at least q entries L[j] = logalpha,(xj), for j=0,...,q-1 and an exponent table E with a first part 412 with respective entries E[j] = i(alpha) for j=0,...,q-2 and a second part 414 immediately subsequent to the first part with respective entries E[j+q-1] = (a<j>) for j=0,...,q-3. A processor 420 provides as the outcome of the multiplication of non-zero elements x, y ∈ Fq an index retrieved from a table entry E[L[i(x)] + L[i(y)]] in the memory.

IPC 1-7

H04L 9/00

IPC 8 full level

G06F 7/72 (2006.01); G06F 1/03 (2006.01)

CPC (source: EP)

G06F 7/724 (2013.01); G06F 1/0307 (2013.01)

Citation (search report)

See references of WO 2004112307A2

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)

WO 2004112307 A2 20041223; **WO 2004112307 A3 20051027**; EP 1636932 A2 20060322

DOCDB simple family (application)

IB 2004050827 W 20040602; EP 04735781 A 20040602