Title (en)

METHOD AND PROCESSOR UNIT FOR IMPLEMENTING A CHARACTERISTIC-2-MULTIPLICATION

Title (de)

VERFAHREN UND PROZESSOR-EINRICHTUNG ZUM IMPLEMENTIEREN EINER CHARAKTERISTIK-2-MULTIPLIKATION

Title (fr)

PROCÉDÉ ET DISPOSITIF PROCESSEUR POUR METTRE EN OEUVRE UNE MULTIPLICATION DE CARACTÉRISTIQUE 2

Publication

EP 2304549 A1 20110406 (DE)

Application

EP 09779527 A 20090522

Priority

- EP 2009056228 W 20090522
- DE 102008033962 A 20080721

Abstract (en)

[origin: WO2010009917A1] The invention relates to a method for implementing a characteristic-2-multiplication of at least two input bit strings, each having a number N of bits, by means of a processor unit suitable for carrying out an integer multiplication, comprising the following steps: a) generating at least one sequence of a number K of zero bits, using K?{1,...,N}, by means of a first transformation of the respective input bit string to at least one predetermined position in the respective input bit string for generating at least one first intermediate bit string; b) linking the at least two first intermediate bit strings by means of the integer multiplication of the processor unit for generating at least one second intermediate bit string; and c) transforming the at least one second intermediate bit string by means of a second transformation for generating a result bit string.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/724 (2013.01 - EP US); G06F 2207/3812 (2013.01 - EP US)

Citation (search report)

See references of WO 2010009917A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

DE 102008033962 A1 20100128; **DE 102008033962 B4 20111124**; CN 102105860 A 20110622; EP 2304549 A1 20110406; JP 2011528810 A 20111124; JP 5449349 B2 20140319; US 2011131395 A1 20110602; US 8732227 B2 20140520; WO 2010009917 A1 20100128

DOCDB simple family (application)

DE 102008033962 A 20080721; CN 200980128600 A 20090522; EP 09779527 A 20090522; EP 2009056228 W 20090522; JP 2011519095 A 20090522; US 200913055218 A 20090522