Title (en)

METHOD FOR SCALARLY MULTIPLYING POINTS ON AN ELLIPTIC CURVE

Title (de)

VERFAHREN ZUR SKALARMULTIPLIKATION VON PUNKTEN AUF EINER ELLIPTISCHEN KURVE

Title (fr)

PROCEDE DE MULTIPLICATION SCALAIRE DE POINTS SUR UNE COURBE ELLIPTIQUE

Publication

EP 1920323 A1 20080514 (DE)

Application

EP 06777699 A 20060711

Priority

- EP 2006064099 W 20060711
- DE 102005041102 A 20050830

Abstract (en)

[origin: WO2007025796A1] The invention relates to a method for scalarly multiplying points on an elliptic curve by a finite expandable field K of a first field F_p of a p>3 characteristic, wherein said characteristic p has low Hamming weight and the expandable field has a polynom F(X) = X^d-2 of order d in the polynomial representation thereof.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/725 (2013.01 - EP US); G06F 2207/7214 (2013.01 - EP US)

Citation (search report)

See references of WO 2007025796A1

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)

WO 2007025796 A1 20070308; CN 101253473 A 20080827; DE 102005041102 A1 20070315; EP 1920323 A1 20080514; US 2009136025 A1 20090528

DOCDB simple family (application)

EP 2006064099 W 20060711; CN 200680031833 A 20060711; DE 102005041102 A 20050830; EP 06777699 A 20060711; US 99118106 A 20060711