Title (en)

METHOD AND DEVICE FOR CALCULATING A POLYNOM MULTIPLICATION, IN PARTICULAR FOR ELLIPTICAL CURVE CRYPTOGRAPHY

Title (de)

VERFAHREN UND VORRICHTUNG ZUM BERECHNEN EINER POLYNOM-MULTIPLIKATION, INSBESONDERE FÜR DIE ELLIPTISCHE KURVEN-KRYPTOGRAPHIE

Title (fr)

PROCEDE ET DISPOSITIF DE CALCUL D'UNE MULTIPLICATION POLYNOME, EN PARTICULIER POUR CRYPTOGRAPHIE CURVILIGNE ELLIPTIQUE

Publication

EP 1859344 A2 20071128 (DE)

Application

EP 06708654 A 20060306

Priority

- EP 2006060494 W 20060306
- EP 05090052 A 20050304
- DE 102005028662 A 20050615
- EP 06708654 A 20060306

Abstract (en)

[origin: DE102005028662A1] The method involves making available coefficients with two polynomials. Each polynomial is fragmented into two or more fragments, being operands for a partial multiplication. The fragments are multiplied in order to receive a partial product. The fragmenting step is recursively implemented, and respective fragments are used as starting points of further fragmenting, until the multiplying step requires a computation step for a partial product of respective fragments only. The selecting and multiplying steps are iterative steps with the received fragments. The partial products are accumulated. An independent claim is included for a device for calculating a polynom multiplication, in particular for elliptical curve cryptography.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/5324 (2013.01 - EP US); **G06F 7/724** (2013.01 - EP US); **G06F 17/10** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); **H04L 9/3093** (2013.01 - EP US); G06F 7/725 (2013.01 - EP US); H04L 2209/122 (2013.01 - EP US); H04L 2209/80 (2013.01 - EP US)

Citation (search report)

See references of WO 2006092448A2

Citation (examination)

- WO 03048918 A1 20030612 - ANALOG DEVICES INC [US]
- ROLF KRAEMER ET AL: "EFFICIENT IMPLEMENTATIONS OF CRYPTOGRAPHIC ROUTINES: A REVIEW AND PERFORMANCE ANALYSIS OF VARIOUS APPROAHCES", COMPUTER SCIENCE REPORTS, BRANDENBURGISCHE UNIVERSITY OF TECHNOLOGY COTTBUS, COTTBUS, DE, 1 January 2004 (2004-01-01), pages 1 - 2, XP001248873

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)

DE 102005028662 A1 20060907; **DE 102005028662 B4 20220602**; EP 1859344 A2 20071128; US 2009136022 A1 20090528; US 8477935 B2 20130702; WO 2006092448 A2 20060908; WO 2006092448 A3 20070329

DOCDB simple family (application)

DE 102005028662 A 20050615; EP 06708654 A 20060306; EP 2006060494 W 20060306; US 88582706 A 20060306