Title (en)

DEVICE FOR PRODUCING EXPONENTIATION CALCULATIONS, AND METHOD FOR PROGRAMMING AND USING SAME

Title (de)

EINRICHTUNG ZUR DURCHFÜHRUNG VON EXPONENTIALBERECHNUNGEN UND VERFAHREN ZUR PROGRAMMIERUNG UND VERWENDUNG DIESER

Title (fr)

DISPOSITIF DESTINE A REALISER DES CALCULS D'EXPONENTIATION, ET PROCEDE DE PROGRAMMATION ET D'UTILISATION DU DISPOSITIF

Publication

EP 1350161 A1 20031008 (FR)

Application

EP 01995782 A 20011221

Priority

- FR 0104182 W 20011221
- FR 0100296 A 20010111

Abstract (en)

[origin: FR2819320A1] The invention concerns an exponentiation calculating device, and a method for programming and using same, for use in particular in the field of cryptology wherein cryptographic algorithms are used in electronic devices such as smart cards. It uses calculating means (2) configured to produce the exponentiation calculations from a addition-subtraction chain C(e) worked out for the exponent e, said addition-subtraction chain being stored in a storage area (6) recordable after its production. Thus, the algorithm can effectively be established from components of the addition-subtraction chain, by post-production programming, without modifying the exponentiation calculating part which can be quenched in a mask read-only-memory, thereby reducing the risks of having to carry out remasking.

IPC 1-7

G06F 7/72; G06F 7/556

IPC 8 full level

G06F 7/556 (2006.01); **G06F 7/72** (2006.01)

CPC (source: EP)

G06F 7/556 (2013.01); **G06F 7/723** (2013.01); G06F 2207/5561 (2013.01)

Citation (search report)

See references of WO 02056171A1

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

FR 2819320 A1 20020712; **FR 2819320 B1 20030808**; EP 1350161 A1 20031008; WO 02056171 A1 20020718

DOCDB simple family (application)

FR 0100296 A 20010111; EP 01995782 A 20011221; FR 0104182 W 20011221