Title (en)

CRYPTOGRAPHIC METHOD FOR SECURELY IMPLEMENTING AN EXPONENTIATION AND RELATED COMPONENT

Title (de)

KRYPTOGRAPHISCHES VERFAHREN ZUM SICHEREN IMPLEMENTIEREN EINER EXPONENTIATION UND DIESBEZÜGLICHE KOMPONENTE

Title (fr)

PROCEDE CRYPTOGRAPHIQUE POUR LA MISE EN OEUVRE SECURISEE D'UNE EXPONENTIATION ET COMPOSANT ASSOCIE

Publication

EP 1904921 A1 20080402 (FR)

Application

EP 06764162 A 20060713

Priority

- EP 2006064228 W 20060713
- FR 0507519 A 20050713

Abstract (en)

[origin: WO2007006810A1] The invention concerns an asymmetrical cryptographic method applied to a message M, characterized in that it includes a private operation which consists in signing or decrypting the message M to obtain a signed or decrypted message s, the private operation being defined based on at least one modular exponentiation EM in the form EM = MA modB, A and B being respectively the exponent and the modular exponentiation EM, and the private operation including the following steps: calculating an intermediate module B*, an intermediate message M* and an intermediate exponent A*, based on B, M and/or A; the intermediate module B* being deterministically calculated and the intermediate message M* being randomly calculated; calculating an intermediate modular exponentiationEM* = M*^{A*} mod B*; calculating the signed or decrypted message s based on the intermediate modular exponentiation EM*. The invention also concerns an electronic component comprising means for implementing said cryptographic method.

IPC 8 full level

G06F 7/72 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

G06F 7/72 (2013.01 - EP US); **G06F 21/556** (2013.01 - EP US); **G06F 21/755** (2017.07 - EP US); **G06F 21/77** (2013.01 - EP US); **H04L 9/003** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); **H04L 9/3249** (2013.01 - EP US)

Citation (search report)

See references of WO 2007006810A1

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)

FR 2888690 A1 20070119; EP 1904921 A1 20080402; US 2009122980 A1 20090514; WO 2007006810 A1 20070118

DOCDB simple family (application)

FR 0507519 A 20050713; EP 06764162 A 20060713; EP 2006064228 W 20060713; US 98875006 A 20060713