Title (en)

DEVICE AND METHOD FOR CALCULATING THE RESULT OF A MODULAR EXPONENTIATION

Title (de)

VORRICHTUNG UND VERFAHREN ZUM BERECHNEN EINES ERGEBNISSES EINER MODULAREN EXPONENTIATION

Title (fr)

DISPOSITIF ET PROCEDE POUR CALCULER LE RESULTAT D'UNE EXPONENTIATION MODULAIRE

Publication

EP 1423786 A2 20040602 (DE)

Application

EP 02797920 A 20020822

Priority

- DE 10143728 A 20010906
- EP 0209405 W 20020822

Abstract (en)

[origin: WO03023605A2] The invention relates to a device for calculating the result of a modular exponentiation based on the Chinese Remainder Theorem (CRT), whereby two auxiliary exponentiations are calculated by using two auxiliary exponents and two sub-modules. The aim of the invention is to increase the security of the RSA-CRT-calculation against cryptographic attacks. As a result, a randomisation of the auxiliary exponents and/or an alteration of the sub-modules is carried out. The Chinese Remainder Theorem enables secure RSA-decoding or RSA-coding to take place by means of the calculation time efficiency.

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/723 (2013.01 - EP US); **H04L 9/004** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); G06F 2207/7242 (2013.01 - EP US); G06F 2207/7247 (2013.01 - EP US); G06F 2207/7271 (2013.01 - EP US)

Citation (search report)

See references of WO 03023605A2

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 03023605 A2 20030320; **WO 03023605 A3 20040401**; CN 1554047 A 20041208; DE 10143728 A1 20030403; DE 10143728 B4 20040902; EP 1423786 A2 20040602; US 2004215685 A1 20041028; US 7248700 B2 20070724

DOCDB simple family (application)

EP 0209405 W 20020822; CN 02817557 A 20020822; DE 10143728 A 20010906; EP 02797920 A 20020822; US 78937304 A 20040227