Title (en)

MODULAR EXPONENTIATION WITH RANDOMIZED EXPONENTS

Title (de)

MODULARE EXPONENTIATION MIT RANDOMISIERTEN EXPONENTEN

Title (fr)

EXPONENTIATION MODULAIRE AU MOYEN D'UN EXPOSANT RANDOMISE

Publication

EP 1590731 A2 20051102 (DE)

Application

EP 04704224 A 20040122

Priority

- EP 2004000522 W 20040122
- DE 10304451 A 20030204

Abstract (en)

[origin: WO2004070497A2] In order to determine a result of a modular exponentiation, a randomization auxiliary number based on the product of the public key and of the private key is set to less than "1" in order to randomize the exponent. This randomization auxiliary number can be derived without special functionalities from the private RSA data record. This enables an low-effort exponent randomization to be universally carried out for each security protocol in order to carry out a digital signature that is secure from side channel attacks.

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP KR US)

G06F 7/723 (2013.01 - EP US); **H04L 9/003** (2013.01 - EP US); **H04L 9/0656** (2013.01 - KR); **H04L 9/14** (2013.01 - KR); **H04L 9/30** (2013.01 - EP KR US); G06F 2207/7257 (2013.01 - EP US); H04L 2209/08 (2013.01 - EP US)

Citation (search report)

See references of WO 2004070497A2

Designated contracting state (EPC)

DE FR

DOCDB simple family (publication)

WO 2004070497 A2 20040819; **WO 2004070497 A3 20050106**; DE 10304451 B3 20040902; EP 1590731 A2 20051102; KR 100731387 B1 20070621; KR 20050106416 A 20051109; US 2007064930 A1 20070322; US 7908641 B2 20110315

DOCDB simple family (application)

EP 2004000522 W 20040122; DE 10304451 A 20030204; EP 04704224 A 20040122; KR 20057014395 A 20050804; US 19535005 A 20050801