Title (en)

SECRET RSA ENCRYPTION EXPONENT THAT CAN BE PROTECTED AGAINST ACCESS VIOLATION

Title (de)

GEGEN AUSSPÄHUNG SCHÜTZBARER GEHEIMER RSA VERSCHLÜSSELUNGSEXPONENT

Title (fr)

EXPOSANT DE CHIFFREMENT RSA SECRET POUVANT ÊTRE PROTÉGÉ CONTRE L'ESPIONNAGE

Publication

EP 2759090 A1 20140730 (DE)

Application

EP 12783498 A 20120917

Priority

- DE 102011115082 A 20110919
- EP 2012003872 W 20120917

Abstract (en)

[origin: WO2013041200A1] The invention relates to a method for generating a secret RSA decryption exponent d which can be protected against access violation in a processor, having the following steps: a) selecting a construction number z; b) selecting two RSA prime numbers p, q dependent on the selected construction number z; c) calculating the RSA modulus n = p s q; d) selecting a public RSA encryption exponent e; and e) calculating an (unmasked) RSA decryption exponent d using the selected construction number z. The decryption exponent d is masked into a protected masked decryption exponent d' by: f) selecting a masking number r; and g) calculating the masked RSA decryption exponent d' using the selected construction number z.

IPC 8 full level

H04L 9/30 (2006.01); **H04L 9/00** (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP)

G06F 7/723 (2013.01); **H04L 9/003** (2013.01); **H04L 9/0861** (2013.01); **H04L 9/302** (2013.01); G06F 2207/7257 (2013.01); H04L 2209/046 (2013.01)

Citation (search report)

See references of WO 2013041200A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

DE 102011115082 A1 20130321; EP 2759090 A1 20140730; WO 2013041200 A1 20130328

DOCDB simple family (application)

DE 102011115082 A 20110919; EP 12783498 A 20120917; EP 2012003872 W 20120917