Title (en)

MONTGOMERY-BASED MODULAR EXPONENTIATION SECURED AGAINST HIDDEN CHANNEL ATTACKS

Title (de)

AUF MONTGOMERY BASIERENDE MODULARE EXPONENTIERUNG MIT SICHERUNG VOR VERBORGENEN KANALATTACKEN

Title (fr)

MISE A LA PUISSANCE MODULAIRE SELON MONTGOMERY SECURISEE CONTRE LES ATTAQUES A CANAUX CACHES

Publication

EP 2162820 A1 20100317 (FR)

Application

EP 08749996 A 20080502

Priority

- EP 2008055427 W 20080502
- EP 07301194 A 20070629
- EP 08749996 A 20080502

Abstract (en)

[origin: EP2015171A1] The method involves drawing of a random value, and initializing variables with the aid of the random value and by utilizing a chosen module and a Montgomery variable. An algorithm enabling a loop invariant to be retained is applied by virtue of properties of a Montgomery multiplier. A result is unmasked to obtain a signature of a message.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/728 (2013.01 - EP US); **H04L 9/003** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); G06F 7/723 (2013.01 - EP US); G06F 2207/7219 (2013.01 - EP US); H04L 2209/046 (2013.01 - EP US)

Citation (search report)

See references of WO 2009003740A1

Designated contracting state (EPC)

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

Designated extension state (EPC)

AL BA MK RS

DOCDB simple family (publication)

EP 2015171 A1 20090114; EP 2162820 A1 20100317; US 2010177887 A1 20100715; WO 2009003740 A1 20090108

DOCDB simple family (application)

EP 07301194 A 20070629; EP 08749996 A 20080502; EP 2008055427 W 20080502; US 66689208 A 20080502