Title (en)

DETERMINATION OF A DIVISION REMAINDER AND DETECTION OF PRIME NUMBER CANDIDATES FOR A CRYPTOGRAPHIC APPLICATION

Title (de)

BESTIMMEN EINES DIVISIONSRESTS DURCH MINDESTENS EINE MONTGOMERY-OPERATION UND ERMITTELN VON PRIMZAHLKANDIDATEN FÜR EINE KRYPTOGRAPHISCHE ANWENDUNG

Title (fr)

DÉTERMINATION D'UN RESTE D'UNE DIVISION ET DE CANDIDATS POUR LES NOMBRES PREMIERS POUR APPLICATION CRYPTOGRAPHIQUE

Publication

EP 2772005 A2 20140903 (DE)

Application

EP 12787360 A 20121025

Priority

- DE 102011117219 A 20111028
- EP 2012004476 W 20121025

Abstract (en)

[origin: WO2013060466A2] The invention relates to a method for determining the division remainder of a first value (b) modulo of a second value (p'), in which a first Montgomery multiplication is performed with the first value (b) as one of the factors and the second value (p') as a modulus (74.1), a correction factor is determined (74.2), and a second Montgomery multiplication is performed with the result of the first Montgomery multiplication as one of the factors and the correction factor as the other factor and the second value (p') as a modulus (74.3). In a method for determining prime number candidates, a basic value (b) is determined for a sieve, and several sieve passes are carried out in which in each case a marking value (p') is determined (72) and multiples of the marking value (p') are marked in the sieve as composite numbers, wherein, in each sieve pass, a division remainder of the basic value (b) modulo of the marking value (p') is determined by means of a remainder determination method (74) that involves at least one Montgomery operation. A device and computer program product have the corresponding characteristics. The mentioned methods can be efficiently implemented on suitable platforms.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP US)

G06F 7/72 (2013.01 - EP US); **G06F 7/728** (2013.01 - EP US); **H04L 9/14** (2013.01 - US); **H04L 9/3033** (2013.01 - EP US); G06F 2207/7204 (2013.01 - EP US)

Citation (search report)

See references of WO 2013060466A2

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 102011117219 A1 20130502; CN 104012029 A 20140827; EP 2772005 A2 20140903; US 2014286488 A1 20140925; WO 2013060466 A2 20130502; WO 2013060466 A3 20131003

DOCDB simple family (application)

DE 102011117219 A 20111028; CN 201280064238 A 20121025; EP 12787360 A 20121025; EP 2012004476 W 20121025; US 201214354254 A 20121025