Title (en)

METHOD FOR GENERATING PRIME NUMBERS PROVEN SUITABLE FOR CHIP CARDS

Title (de)

VERFAHREN ZUR ERZEUGUNG VON NACHGEWIESENERMASSEN FÜR CHIPKARTEN GEEIGNETE PRIMZAHLEN

Title (fr)

PROCEDE DE GENERATION DE NOMBRES PREMIERS PROUVES ADAPTE AUX CARTES A PUCE

Publication

EP 2791784 A1 20141022 (FR)

Application

EP 12815734 A 20121212

Priority

- FR 1161739 A 20111215
- FR 1161740 A 20111215
- FR 1161741 A 20111215
- FR 1161742 A 20111215
- FR 1201550 A 20120530
- FR 2012052902 W 20121212

Abstract (en)

[origin: WO2013088065A1] The invention relates to a prime number generation method implemented in an electronic device (DV). The method includes steps of generating a prime number from another prime number via the formula Pr = 2P × R + 1, wherein P is a prime number having a bit number less than that of the potential prime number and R is an integer, and using the Pocklington primality test on the candidate prime number. The candidate prime number is proven to be prime when passing the Pocklington test. According to the invention, the size in number of bits of the candidate prime number is equal to three times the size of the prime number (P) to a nearest whole unit, the generated candidate prime number being kept as a candidate prime number only if the quotient (U) from the integer division of the integer (R) by the prime number is odd.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/58 (2013.01 - US); **G06F 7/72** (2013.01 - EP US); **G06F 17/11** (2013.01 - US); **H04L 9/0816** (2013.01 - US); **H04L 9/0869** (2013.01 - US); G06F 2207/7204 (2013.01 - EP US); H04L 2209/24 (2013.01 - US)

Citation (search report)

See references of WO 2013088066A1

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)

WO 2013088065 A1 20130620; CN 104067217 A 20140924; EP 2791783 A1 20141022; EP 2791783 B1 20190417; EP 2791784 A1 20141022; IN 4637CHN2014 A 20150918; US 2014355758 A1 20141204; US 2014358980 A1 20141204; US 9577826 B2 20170221; US 9596080 B2 20170314; WO 2013088066 A1 20130620

DOCDB simple family (application)

FR 2012052901 W 20121212; CN 201280062261 A 20121212; EP 12815733 A 20121212; EP 12815734 A 20121212; FR 2012052902 W 20121212; IN 4637CHN2014 A 20140619; US 201214365671 A 20121212; US 201214365899 A 20121212