Title (en)

CRYPTOGRAPHIC METHOD WITH ELLIPTICAL CURVES

Title (de)

KRYPTOGRAPHISCHES VERFAHREN MIT ELLIPTISCHEN KURVEN

Title (fr)

PROCEDE CRYPTOGRAPHIQUE À COURBES ELLIPTIQUES

Publication

EP 1997000 A1 20081203 (DE)

Application

EP 07726643 A 20070306

Priority

- EP 2007052075 W 20070306
- DE 102006013515 A 20060323

Abstract (en)

[origin: WO2007107450A1] The invention relates to a method for determining an elliptical curve, suitable for a cryptographic method, comprising the following steps: (a) an elliptical curve to be tested is prepared; (b) the order of a twisted elliptical curve associated with the elliptical curve to be tested is determined; (c) it is automatically checked whether the order of the twisted elliptical curve is a strong prime number; and (d) if the order of the twisted elliptical curve is a strong prime number, the elliptical curve to be tested is selected as an elliptical curve suitable for cryptographical methods.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP KR US)

G06F 3/03 (2013.01 - KR); **G06F 7/72** (2013.01 - KR); **G06F 7/725** (2013.01 - EP US); **G06F 21/00** (2013.01 - KR); G06F 2207/7219 (2013.01 - EP US)

Citation (search report)

See references of WO 2007107450A1

Citation (examination)

BROWN D R L ET AL: "The Static Diffie-Hellman Problem", 23 June 2005 (2005-06-23), pages 1 - 17, XP002533452, Retrieved from the Internet <URL:http://eprint.iacr.org/2004/306.ps>

Designated contracting state (EPC)

DE ES FR GB IT

DOCDB simple family (publication)

WO 2007107450 A1 20070927; CN 101410792 A 20090415; CN 101410792 B 20130306; DE 102006013515 A1 20071004; EP 1997000 A1 20081203; JP 2009531726 A 20090903; JP 2012123426 A 20120628; KR 101391216 B1 20140502; KR 20080111089 A 20081222; US 2009285388 A1 20091119; US 8582761 B2 20131112

DOCDB simple family (application)

EP 2007052075 W 20070306; CN 200780010399 A 20070306; DE 102006013515 A 20060323; EP 07726643 A 20070306; JP 2009501996 A 20070306; JP 2012069762 A 20120326; KR 20087025841 A 20081022; US 22548007 A 20070306