Title (en)

METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A SECURE PORTABLE OBJECT USING SAID METHOD

Title (de)

VERFAHREN ZUM ERZEUGEN ELEKTRONISCHER SCHLÜSSEL FÜR EIN KRYPTOGRAPHIEVERFAHREN MIT ÖFFENTLICHEN SCHLÜSSELN UND DAS VERFAHREN VERWENDENDES SICHERES TRAGBARES OBJEKT

Title (fr)

PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCEDE

Publication

EP 1523823 A2 20050420 (FR)

Application

EP 03760742 A 20030618

Priority

- FR 0301871 W 20030618
- FR 0207688 A 20020619

Abstract (en)

[origin: WO2004002058A2] The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

IPC 1-7

H04L 9/30

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/08** (2006.01); **G06F 7/72** (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

H04L 9/0861 (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); H04L 2209/30 (2013.01 - EP US); H04L 2209/80 (2013.01 - EP US)

Citation (search report)

See references of WO 2004002058A2

Citation (examination)

- JOYCE M ET AL: "EFFICIENT GENERATION OF PRIME NUMBERS", CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 2ND INTERNATIONAL WORKSHOP, CHES 2000, WORCHESTER, MA, AUG. 17 - 18, 2000 PROCEEDINGS; [LECTURE NOTES IN COMPUTER SCIENCE], BERLIN : SPRINGER, DE, vol. VOL. 1965, 17 August 2000 (2000-08-17), pages 340 - 354, XP001049142, ISBN: 978-3-540-41455-1
- MARC JOYE ET AL: "Constructive Methods for the Generation of Prime Numbers (*** Submission to NESSIE ***)", 13 September 2001 (2001-09-13), XP055190231, Retrieved from the Internet <URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.1212&rep=rep1&type=pdf> [retrieved on 20150519]

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

DOCDB simple family (publication)

FR 2841411 A1 20031226; **FR 2841411 B1 20041029**; AU 2003258815 A1 20040106; EP 1523823 A2 20050420; JP 2005530212 A 20051006; JP 4765108 B2 20110907; US 2005226411 A1 20051013; WO 2004002058 A2 20031231; WO 2004002058 A3 20040415

DOCDB simple family (application)

FR 0207688 A 20020619; AU 2003258815 A 20030618; EP 03760742 A 20030618; FR 0301871 W 20030618; JP 2004514946 A 20030618; US 51863904 A 20041220