Title (en)

CRYPTOGRAPHIC METHOD FOR DISTRIBUTING LOAD AMONG SEVERAL ENTITIES AND DEVICES THEREFOR

Title (de)

KRYPTOGRAPHISCHES VERFAHREN ZUR VERTEILUNG DER LAST ZWISCHEN MEHREREN EINHEITEN UND VORRICHTUNGEN ZUR AUSFÜHRUNG DES VERFAHRENS

Title (fr)

PROCEDE CRYPTOGRAPHIQUE PERMETTANT DE REPARTIR LA CHARGE ENTRE PLUSIEURS ENTITES ET DISPOSITIFS POUR METTRE EN OEUVRE CE PROCEDE

Publication

EP 1456998 A1 20040915 (FR)

Application

EP 02799095 A 20021216

Priority

- FR 0204366 W 20021216
- FR 0116789 A 20011221

Abstract (en)

[origin: WO03055134A1] The invention concerns a cryptographic method whereby a second entity (B) verifies by means of a public key, a proof provided by a first entity (A), which consists in the generation by the first entity (A) of a first random number r much higher than any first integer s included in a private key kept secret by the first entity (A). The first entity (A) generates a first element of proof resulting from a modulo n exponentiation of a first integer G included or not in said public key and whereof the exponent is the first random number r. In combination with the first element of proof, a so-called common number, is generated so that the second entity (B) and the first entity (A) should have knowledge of the common number. The first entity (A) generates an image y of said private key by linear combination of the first random number r and of at least a first private key integer s. At least a multiplicative coefficient of the linear combination is said common number. Any one entity generates a second element of proof Y equal to a power modulo n of a second integer G included or not in said public key and whereof the exponent is the image y of said common number, and sends the second element of proof Y to the first entity (B). The second entity (B) verifies whether the first element of proof is in conformity with a product modulo n of a power of the second element of proof Y whereof the exponent is a third integer e and of a power of a fourth integer v included in said public key whereof the exponent is said common number c.

IPC 1-7

H04L 9/32

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP KR US)

H04L 9/00 (2013.01 - KR); **H04L 9/302** (2013.01 - EP US); **H04L 9/32** (2013.01 - KR); **H04L 9/3218** (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US); H04L 2209/80 (2013.01 - EP US)

Citation (search report)

See references of WO 03055134A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 03055134 A1 20030703; **WO 03055134 A9 20040715**; AU 2002364321 A1 20030709; CN 1618200 A 20050518; CN 1618200 B 20100512; EP 1456998 A1 20040915; FR 2834153 A1 20030627; FR 2834153 B1 20040423; JP 2005513564 A 20050512; KR 100971038 B1 20100720; KR 20040096509 A 20041116; US 2005220298 A1 20051006; US 7382875 B2 20080603

DOCDB simple family (application)

FR 0204366 W 20021216; AU 2002364321 A 20021216; CN 02827791 A 20021216; EP 02799095 A 20021216; FR 0116789 A 20011221; JP 2003555732 A 20021216; KR 20047009924 A 20021216; US 49956304 A 20040621