Title (en)

METHOD FOR GENERATING AN ELECTRONIC KEY FROM A PRIME NUMBER CONTAINED IN A SPECIFIC INTERVAL AND DEVICE THEREFOR

Title (de)

VERFAHREN ZUR ERZEUGUNG EINES ELEKTRONISCHEN SCHLÜSSLES AUS EINER IN EINEM BESTIMMTEN INTERVALL BEFINDLICHEN PRIMZAHL UND VORRICHTUNG ZUR AUSFÜHRUNG DES VERFAHRENS

Title (fr)

PROCEDE DE GENERATION D'UNE CLE ELECTRONIQUE A PARTIR D'UN NOMBRE PREMIER COMPRIS DANS UN INTERVALLE DETERMINE ET DISPOSITIF DE MISE EN OEUVRE DU PROCEDE

Publication

EP 1302021 A1 20030416 (FR)

Application

EP 01947562 A 20010621

Priority

- FR 0101948 W 20010621
- FR 0008994 A 20000710

Abstract (en)

[origin: WO0205483A1] The invention concerns a method for generating an electronic key from a prime number q contained in a specific interval of positive integers (W>m<, W>M<). Said method comprises the following operations: a) selecting a positive integer eta , eta being the product of the k first prime numbers, with k as maximum so that there exist two positive integers epsilon >m< and epsilon >M< such that epsilon >m <is the higher roundoff of W>m</ eta , and epsilon >M< is the lower roundoff of (W>M<-W>m<)/ eta , calculating PI = epsilon >M<. eta and rho = epsilon >m<. eta , generating two positive integers a and c belonging to the multiplicative group Z*> PI < of integers modulo PI , with prime c with PI , calculating q = c + rho ; b) testing primality nature of q; c) if primality is verified, q is stored; d) otherwise: updating c by calculating a.c mod PI , repeating the preceding operations as from b) with the new value q = c+ rho . The invention is applicable to cryptography.

IPC 1-7

H04L 9/30

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

H04L 9/3033 (2013.01 - EP US); H04L 2209/805 (2013.01 - EP US)

Citation (search report)

See references of WO 0205483A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 0205483 A1 20020117; AU 6922101 A 20020121; CN 1449609 A 20031015; EP 1302021 A1 20030416; FR 2811442 A1 20020111; FR 2811442 B1 20020913; JP 2004502984 A 20040129; JP 3833175 B2 20061011; US 2004114757 A1 20040617

DOCDB simple family (application)

FR 0101948 W 20010621; AU 6922101 A 20010621; CN 01814877 A 20010621; EP 01947562 A 20010621; FR 0008994 A 20000710; JP 2002509226 A 20010621; US 31115303 A 20030424