Title (en)

COUNTERMEASURE METHOD IN AN ELECTRIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM

Title (de)

GEGENMASSNAHMEVERFAHREN IN EINER ELEKTRONISCHEN KOMPONENTE, WELCHE EINE KRYPTOGRAPHISCHEN ALGORITHMUS MIT ÖFFENTLICHEM SCHLÜSSEL AUF BASIS EINER ELLIPTISCHEN KURVE EINSETZT

Title (fr)

PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

Publication

EP 1166495 A1 20020102 (FR)

Application

EP 00915215 A 20000322

Priority

- FR 0000723 W 20000322
- FR 9903920 A 19990326

Abstract (en)

[origin: FR2791496A1] The invention relates to a countermeasure method in an electronic component implementing an elliptical curve based public key cryptography algorithm, comprising the calculation of a new decryption integer d' such as the decryption of an encrypted message with the aid of a decryption algorithm on the basis of a private key d and the number of points n of said elliptical curve whereby the same result is achieved with d' as with d, by performing the operation Q=d*P, whereby P is a point of the curve. The inventive measure is characterized in that it comprises four steps: 1) a security parameter s is determined, whereby in practice it is impossible to take s as a neighbour of 30, 2) a random number k ranging from 0-21s is drawn, 3) the integer d'=d+k*n is calculated, 4) Q=d'.P is calculated.

IPC 1-7

H04L 9/30

IPC 8 full level

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

CPC (source: EP US)

G06F 7/725 (2013.01 - EP US); **H04L 9/003** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); G06F 2207/7238 (2013.01 - EP US); G06F 2207/7247 (2013.01 - EP US); G06F 2207/7257 (2013.01 - EP US); H04L 2209/046 (2013.01 - EP US); H04L 2209/08 (2013.01 - EP US)

Citation (search report)

See references of WO 0059157A1

Cited by

EP2326041A1; WO2011061263A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

FR 2791496 A1 20000929; **FR 2791496 B1 20011019**; AU 3660300 A 20001016; CN 1218531 C 20050907; CN 1345496 A 20020417; EP 1166495 A1 20020102; JP 2002540484 A 20021126; MX PA01009402 A 20020604; US 7286666 B1 20071023; WO 0059157 A1 20001005

DOCDB simple family (application)

FR 9903920 A 19990326; AU 3660300 A 20000322; CN 00805519 A 20000322; EP 00915215 A 20000322; FR 0000723 W 20000322; JP 2000608546 A 20000322; MX PA01009402 A 20000322; US 93739700 A 20000322