Title (en)

SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST POWER ATTACKS

Title (de)

VERFAHREN ZUR SICHERUNG EINER AUF MODULARER POTENZIERUNG BASIERENDEN ELEKTRONISCHEN KRYPTOANLAGE GEGEN ANGRIFFE MITTELS LEISTUNGSANALYSE

Title (fr)

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A BASE D'EXPONENTIATION MODULAIRE CONTRE LES ATTAQUES PAR ANALYSE DE PUISSANCE

Publication

EP 1639447 A1 20060329 (FR)

Application

EP 00971508 A 20001026

Priority

- FR 0002978 W 20001026
- FR 9913507 A 19991028

Abstract (en)

[origin: WO0131436A1] The invention concerns a security method for an electronic assembly implementing a cryptographic computation process using a modular exponentiation of a quantity (x), said modular exponentiation utilising a secret exponent (d). The invention is characterised in that it consists in breaking down said secret exponent into a plurality of k unpredictable values (d1, d2, ..., dk) whereof the sum is equal to said secret exponent.

IPC 1-7

G06F 7/72

IPC 8 full level

H04L 9/10 (2006.01); **G06F 7/72** (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP US)

G06F 7/723 (2013.01 - EP US); G06F 2207/7242 (2013.01 - EP US)

Citation (search report)

See references of WO 0131436A1

Citation (examination)

TSUTOMU ET AL: "Speeding Up Secret Computations with Insecure Auxiliary Devices", ADVANCES IN CRYPTOLOGY, PROCEEDINGS OF THE CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHY, 21 August 1998 (1998-08-21) - 25 August 1988 (1988-08-25), Berlin, pages 497 - 506, XP000345652

Cited by

CN102521544A

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)

WO 0131436 A1 20010503; EP 1639447 A1 20060329; FR 2800478 A1 20010504; FR 2800478 B1 20011130; JP 2003513491 A 20030408; US 6973190 B1 20051206

DOCDB simple family (application)

FR 0002978 W 20001026; EP 00971508 A 20001026; FR 9913507 A 19991028; JP 2001533507 A 20001026; US 86943501 A 20010628