Title (en)

METHOD FOR MAKING SECURE AN ELECTRONIC ENTITY WITH ENCRYPTED ACCESS

Title (de)

VERFAHREN ZUR SICHERUNG EINER ELEKTRONISCHEN VORRICHTUNG MIT VERSCHLÜSSELTEM ZUGANG

Title (fr)

PROCEDE DE SECURISATION D UNE ENTITE ELECTRONIQUE A ACCES CR YPTE

Publication

**EP 1493242 A1 20050105 (FR)**

Application

**EP 03740554 A 20030402**

Priority

- FR 0301032 W 20030402
- FR 0204341 A 20020408

Abstract (en)

[origin: WO03085881A1] The invention concerns a method for protecting an electronic entity with encrypted access, against DFA (Differential Fault Analysis) attacks which consists in: storing the result of a selected step (Rm, Kn) of an iterative process forming part of the cryptographic algorithm and in performing once more at least part of the steps of said iterative process up to a new computation of a result corresponding to the one which has been stored, comparing the two results and denying distribution of an encrypted message (MC) if they are different.

IPC 1-7

**H04L 9/06**

IPC 8 full level

**H04L 9/10** (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP US)

**H04L 9/004** (2013.01 - EP US); **H04L 9/0618** (2013.01 - EP US); H04L 2209/24 (2013.01 - EP US)

Citation (search report)

See references of WO 03085881A1

Citation (examination)

- DAEMEN J ET AL: "Specification of Rijndael", 1 January 2002, THE DESIGN OF RIJNDAEL. AES - THE ADVANCED ENCRYPTION STANDARD, SPRINGER, PAGE(S) 31 - 51, ISBN: 978-3-540-42580-9, XP007919936
- BIHAM E ET AL: "DIFFERENTIAL FAULT ANALYSIS OF SECRET KEY CRYPTOSYSTEMS", ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997; [PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO)], BERLIN, SPRINGER, DE, vol. CONF. 17, 17 August 1997 (1997-08-17), pages 513 - 526, XP001060384, ISBN: 978-3-540-63384-6

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)

**WO 03085881 A1 20031016**; AU 2003260714 A1 20031020; CA 2480896 A1 20031016; CA 2480896 C 20121030; EP 1493242 A1 20050105; FR 2838262 A1 20031010; FR 2838262 B1 20040730; JP 2005522912 A 20050728; JP 2011103686 A 20110526; US 2006104438 A1 20060518; US 2010322421 A1 20101223; US 7796750 B2 20100914; US 8180046 B2 20120515

DOCDB simple family (application)

**FR 0301032 W 20030402**; AU 2003260714 A 20030402; CA 2480896 A 20030402; EP 03740554 A 20030402; FR 0204341 A 20020408; JP 2003582947 A 20030402; JP 2011000207 A 20110104; US 51028405 A 20051109; US 85263710 A 20100809