



(11)

EP 1 922 837 B8

(12)

KORRIGIERTE EUROPÄISCHE PATENTSCHRIFT

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 B1)
Korrekturen, siehe
Bibliographie INID code(s) 73

(51) Int Cl.:
H04L 9/30 ^(2006.01) **G06F 7/72** ^(2006.01)

(86) Internationale Anmeldenummer:
PCT/EP2006/064655

(48) Corrigendum ausgegeben am:
21.12.2016 Patentblatt 2016/51

(87) Internationale Veröffentlichungsnummer:
WO 2007/028669 (15.03.2007 Gazette 2007/11)

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
31.08.2016 Patentblatt 2016/35

(21) Anmeldenummer: **06792567.7**

(22) Anmeldetag: **26.07.2006**

(54) **VERFAHREN ZUM SICHEREN VER- ODER ENTSCHLÜSSELN EINER NACHRICHT**

METHOD FOR SECURELY ENCRYPTING OR DECRYPTING A MESSAGE

PROCEDE DE CODAGE OU DECODAGE SECURISE D'UN MESSAGE

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR**

(30) Priorität: **06.09.2005 DE 102005042339**

(43) Veröffentlichungstag der Anmeldung:
21.05.2008 Patentblatt 2008/21

(73) Patentinhaber: **Siemens Aktiengesellschaft
80333 München (DE)**

(72) Erfinder:
• **KARGL, Anton**
80639 München (DE)
• **MEYER, Bernd**
81739 München (DE)
• **BRAUN, Michael**
81825 München (DE)

(56) Entgegenhaltungen:

- **CHEVALLIER-MAMES B: "Self-randomized exponentiation algorithms" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, Bd. 2964, 27. Februar 2004 (2004-02-27), Seiten 236-249, XP002297836 ISSN: 0302-9743**
- **PIERRE-ALAIN FOUQUE ET AL: "Defeating Countermeasures Based on Randomized BSD Representations" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2004, 8. Juli 2004 (2004-07-08), Seiten 312-327, XP019009374 Cambridge, MA, USA**
- **ITOH K ET AL: "DPA COUNTERMEASURES BY IMPROVING THE WINDOW METHOD" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, 13. August 2002 (2002-08-13), Seiten 303-317, XP001160529**
- **CHEVALLIER-MAMES B ET AL: "Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity" IEEE TRANSACTIONS ON COMPUTERS, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, Bd. 53, Nr. 6, Juni 2004 (2004-06), Seiten 760-768, XP002356344 ISSN: 0018-9340**

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 1 922 837 B8

- **CHANGKYUN KIM ET AL: "A Secure and Practical CRT-Based RSA to Resist Side Channel Attacks"**
LNCS INTERNATIONAL CONFERENCE, ASSISI,
26. April 2004 (2004-04-26), Seiten 150-158,
XP019006751
- **Kouichi Itoh ET AL: "A Practical Countermeasure
against Address-Bit Differential Power Analysis"**
In: "LECTURE NOTES IN COMPUTER SCIENCE",
1 January 2003 (2003-01-01), Springer Berlin
Heidelberg, Berlin, Heidelberg, XP055155620,
ISSN: 0302-9743 ISBN: 978-3-54-045234-8 vol.
2779, pages 382-396, DOI:
10.1007/978-3-540-45238-6_30,