(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 616 406 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 54

(48) Corrigendum issued on:
21.12.2016 Bulletin 2016/51

(45) Date of publication and mention of the grant of the patent:
05.10.2016 Bulletin 2016/40

(21) Application number: **04718163.1**

(22) Date of filing: **05.03.2004**

(51) Int Cl.:
H04L 9/32 *(2006.01)*

(86) International application number:
PCT/US2004/007040

(87) International publication number:
WO 2004/095773 (04.11.2004 Gazette 2004/45)

(54) **ESTABLISHING TRUST WITHOUT REVEALING IDENTITY**

VERTRAUENSCHAFFUNG OHNE DIE IDENTITÄT OFFEN ZU LEGEN

ETABLIR LA CONFIANCE SANS DEVOILER L'IDENTITE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR

(30) Priority: **11.04.2003 US 412366**

(43) Date of publication of application:
18.01.2006 Bulletin 2006/03

(73) Proprietor: **Intel Corporation**
Santa Clara, CA 95054 (US)

(72) Inventor: **BRICKELL, Ernie**
Portland, OR 97210 (US)

(74) Representative: **Beresford, Keith Denis Lewis**
Beresford Crump LLP
16 High Holborn
London WC1V 6BX (GB)

(56) References cited:
FR-A- 2 620 248
FR-A- 2 700 430
FR-A- 2 714 780
FR-A- 2 742 618
FR-A- 2 752 122
FR-A- 2 763 452
FR-A- 2 830 147
US-B1- 6 473 508

- **GILLES ZEMOR: "Cours de cryptography" November 2000 (2000-11), CASSINI , PARIS , XP002313885 ISBN: 2-844225-020-6 page 165 - page 173**
- **M. PRABHAKARAN, A. SAHAI: "Concurrent Zero Knowledge Proofs with Logarithmic Round-Complexity"[Online] 6 May 2002 (2002-05-06), pages A,1-19, XP002313883 Retrieved from the Internet: URL:http://eprint.iacr.org/2002/055.pdf> [retrieved on 2004-09-22]**
- **D. MICCIANCIO, E. PETRANK: "Efficient and Concurrent Zero-Knowledge from any public coin HVZK protocol"[Online] 8 July 2002 (2002-07-08), pages 1-20, XP002313884 Retrieved from the Internet: URL:http://eprint.iacr.org/2002/090.pdf> [retrieved on 2004-09-22]**
- **ERNIE BRICKELL ET AL: "Direct Anonymous Attestation", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20040821:115324, 20 August 2004 (2004-08-20), pages 1-28, XP061000928, [retrieved on 2004-08-20]**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- CAMENISCH J ET AL: "Dynamic accumulators and application to efficient revocation of anonymous credentials", SECURITY IN COMMUNICATION NETWORKS : THIRD INTERNATIONAL CONFERENCE ; REVISED PAPERS / SCN 2002, AMALFI, ITALY, SEPTEMBER 11 - 13, 2002; [LECTURE NOTES IN COMPUTER SCIENCE , ISSN 0302-9743], SPRINGER VERLAG, DE, vol. 2442, 1 February 2002 (2002-02-01), pages 61-76, XP002391625, DOI: 10.1007/3-540-45708-9_5 ISBN: 978-3-540-24128-7
- "TRUSTED COMPUTING PLATFORM ALLIANCE (TCPA) MAIN SPECIFICATION VERSION 1.1B", INTERNET CITATION, 22 February 2002 (2002-02-22), XP002304627, Retrieved from the Internet: URL:http://www.trustedcomputinggroup.org/downloads/Maijn_TCG_Architecture_v1_1b.zip [retrieved on 2004-11-08]
- LANGLOIS ADELINE ET AL: "Lattice-Based Group Signature Scheme with Verifier-Local Revocation", 26 March 2014 (2014-03-26), ADVANCES IN COMMUNICATION NETWORKING : 20TH EUNICE/IFIP EG 6.2, 6.6 INTERNATIONAL WORKSHOP, RENNES, FRANCE, SEPTEMBER 1-5, 2014, REVISED SELECTED PAPERS; [LECTURE NOTES IN COMPUTER SCIENCE , ISSN 1611-3349], SPRINGER VERLAG, DE, PAGE(S) 345 - 361, XP047183556, ISSN: 0302-9743