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

(11) **EP 2 441 207 B8**

(12) **FASCICULE DE BREVET EUROPEEN CORRIGE**

(15) Information de correction:
Version corrigée no 1 (W1 B1)
Corrections, voir
Bibliographie code(s) INID 73

(48) Corrigendum publié le:
05.08.2020 Bulletin 2020/32

(45) Date de publication et mention de la délivrance du brevet:
03.06.2020 Bulletin 2020/23

(21) Numéro de dépôt: **10737992.7**

(22) Date de dépôt: **11.06.2010**

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

(86) Numéro de dépôt international:
PCT/FR2010/051167

(87) Numéro de publication internationale:
WO 2010/142923 (16.12.2010 Gazette 2010/50)

(54) **PROCÉDÉ CRYPTOGRAPHIQUE D'AUTHENTIFICATION ANONYME ET D'IDENTIFICATION SÉPARÉE D'UN UTILISATEUR**

KRYPTOGRAFISCHES VERFAHREN FÜR ANONYME AUTHENTIFIZIERUNG UND SEPARATE IDENTIFIZIERUNG EINES BENUTZERS

CRYPTOGRAPHIC METHOD FOR ANONYMOUS AUTHENTICATION AND SEPARATE IDENTIFICATION OF A USER

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(30) Priorité: **12.06.2009 FR 0953953**

(43) Date de publication de la demande:
18.04.2012 Bulletin 2012/16

(73) Titulaire: **ORANGE**
75015 Paris (FR)

(72) Inventeurs:
- **CANARD, Sébastien**
  F-14000 Caen (FR)
- **JAMBERT, Amandine**
  F-14000 Caen (FR)
- **MALVILLE, Eric**
  F-35760 Saint Grégoire (FR)

(74) Mandataire: **Plasseraud IP**
66, rue de la Chaussée d'Antin
75440 Paris Cedex 09 (FR)

(56) Documents cités:
EP-A2- 1 808 795 WO-A2-2008/149029

- **SEBASTIEN CANARD ET AL: "Trapdoor Sanitizable Signatures and Their Application to Content Protection" 5 juin 2007 (2007-06-05), APPLIED CRYPTOGRAPHY AND NETWORK SECURITY; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 258 - 276 , XP019076275 ISBN: 9783540689133 le document en entier**
- **CHRISTINA BRZUSKA ET AL: "Security of Sanitizable Signatures Revisited" 18 mars 2009 (2009-03-18), PUBLIC KEY CRYPTOGRAPHY Â PKC 2009, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 317 - 336 , XP019115182 ISBN: 9783642004674 alinéas [0002], [0005]**

Printed by Jouve, 75001 PARIS (FR)

(Cont. page suivante)

- **XIAOFENG CHEN ET AL: "Chameleon Hashing Without Key Exposure" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER, DE LNKD-DOI:10.1007/B100936, vol. 3225, 21 septembre 2004 (2004-09-21), pages 87-98, XP007912633 ISSN: 0302-9743**
- **BENOÎT CHEVALLIER-MAMES ED - VICTOR SHOUP: "An Efficient CDH-Based Signature Scheme with a Tight Security Reduction" 1 janvier 2005 (2005-01-01), ADVANCES IN CRYPTOLOGY - CRYPTO 2005 LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 511 - 526 , XP019016572 ISBN: 9783540281146 alinéa [0004]**