



(11)

EP 2 667 371 B8

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

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

(51) Int Cl.:
H04L 9/00 (2006.01)

(86) International application number:
PCT/JP2012/055404

(48) Corrigendum issued on:
07.03.2018 Bulletin 2018/10

(87) International publication number:
WO 2012/121152 (13.09.2012 Gazette 2012/37)

(45) Date of publication and mention
of the grant of the patent:
22.11.2017 Bulletin 2017/47

(21) Application number: **12755320.4**

(22) Date of filing: **02.03.2012**

(54) **PROXY CALCULATION SYSTEM, METHOD, REQUEST DEVICE, AND PROGRAM**

PROXYBERECHNUNGSSYSTEM UND -VERFAHREN, ANFRAGEVORRICHTUNG, UND
PROGRAMM

SYSTÈME, MÉTHODE, DISPOSITIF DE REQUÊTE ET PROGRAMME DE CALCUL PAR
ENTREMETTEUR

(84) Designated Contracting States:
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 RS SE SI SK SM TR

(74) Representative: **MERH-IP Matias Erny Reichl**
Hoffmann
Patentanwälte PartG mbB
Paul-Heyse-Strasse 29
80336 München (DE)

(30) Priority: **04.03.2011 JP 2011047840**

(43) Date of publication of application:
27.11.2013 Bulletin 2013/48

(56) References cited:
JP-A- 2011 053 607

(73) Proprietor: **Nippon Telegraph And Telephone**
Corporation
Tokyo 100-8116 (JP)

• **ELENA GRIGORESCU ET AL: "Local Decoding
and Testing for Homomorphisms", 1 January
2006 (2006-01-01), APPROXIMATION,
RANDOMIZATION, AND COMBINATORIAL
OPTIMIZATION. ALGORITHM MS AND
TECHNIQUES LECTURE NOTES IN COMPUTER
SCIENCE;;LNCS, SPRINGER, BERLIN, DE,
PAGE(S) 375 - 385, XP019039358, ISBN:
978-3-540-38044-3 * section 1 ** section 6 ***

(72) Inventors:
• **YAMAMOTO, Go**
Musashino-shi
Tokyo 180-8585 (JP)
• **KOBAYASHI, Tetsutaro**
Musashino-shi
Tokyo 180-8585 (JP)

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 667 371 B8

- GO YAMAMOTO ET AL: "Ango Module ni Taisuru Jiko Teiseiki [Self-Correctors for Cryptographic modules]", 2011 NEN SYMPOSIUM ON CRYPTOGRAPHY AND INFORMATION SECURITY; THE 2011 SYMPOSIUM ON CRYPTOGRAPHY AND INFORMATION SECURITY; KOKURA, JAPAN; 25-28/01/2011, IEICE, JP, 25 January 2011 (2011-01-25), pages 1-8, XP008172389,
- CHIDA K ET AL: "Batch processing for proofs of partial knowledge and its applications", IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol. E91A, no. 1, 1 January 2008 (2008-01-01), pages 150-159, XP001509989, ISSN: 0916-8508, DOI: 10.1093/IETFEC/E91-A.1.150
- BELLARE M ET AL: "Fast batch verification for modular exponentiation and digital signatures", ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SPRINGER VERLAG, DE, 1 January 1998 (1998-01-01), pages 236-250, XP002204200,
- GO YAMAMOTO ET AL.: 'Ango Module ni Taisuru Jiko Teiseiki' 2011 NEN SYMPOSIUM ON CRYPTOGRAPHY AND INFORMATION SECURITY 25 January 2011, pages 1 - 8, XP008172389
- YUTO KAWAHARA ET AL.: 'Pairing Ango System ni Okeru Jiko Teisei o Mochiita Fukugo Module no Kosei Oyobi Jisso' 2011 NEN SYMPOSIUM ON CRYPTOGRAPHY AND INFORMATION SECURITY 25 January 2011, pages 1 - 8, XP008172390
- KOJICHIDA ET AL.: 'Batch Processing for Proofs of Partial Knowledge and Its Applications' IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES vol. E91-A, no. 1, 01 January 2008, pages 150 - 159, XP001509989
- Manuel Blum ET AL: "Self-testing/correcting with applications to numerical problems", Journal of Computer and System Sciences, vol. 47, no. 3, 1 December 1993 (1993-12-01), pages 549-595, XP055089183, ISSN: 0022-0000, DOI: 10.1016/0022-0000(93)90044-W