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

(11) **EP 2 544 398 B8**

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

(15) Information de correction:
Version corrigée no 1 (W1 B1)
Corrections, voir
Bibliographie code(s) INID 54

(48) Corrigendum publié le:
14.12.2016 Bulletin 2016/50

(45) Date de publication et mention de la délivrance du brevet:
02.09.2015 Bulletin 2015/36

(21) Numéro de dépôt: **12174881.8**

(22) Date de dépôt: **04.07.2012**

(51) Int Cl.:
H04L 9/30 *(2006.01)*

(54) **Procédé de calcul de fonctions d'encodage dans une courbe elliptique et coprocesseur cryptographique correspondant**

Verfahren zur Berechnung einer Kodierungsfunktion in einer elliptischen Kurve, und entsprechender kryptografischer Koprozessor

Method for computing an encoding into an elleptic curve and corresponding cryptographic coprocessor

(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 RS SE SI SK SM TR

(30) Priorité: **04.07.2011 FR 1155992**

(43) Date de publication de la demande:
09.01.2013 Bulletin 2013/02

(73) Titulaire: **Oberthur Technologies**
92700 Colombes (FR)

(72) Inventeurs:
- **Sierra, Yannick**
  92726 NANTERRE CEDEX (FR)
- **Rondepierre, Franck**
  92726 NANTERRE CEDEX (FR)

(74) Mandataire: **Orsini, Fabienne et al**
Jacobacci Coralis Harle
14/16, rue Ballu
75009 Paris (FR)

(56) Documents cités:
- **THOMAS ICART: "How to Hash into Elliptic Curves", 16 août 2009 (2009-08-16), ADVANCES IN CRYPTOLOGY - CRYPTO 2009, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 303 - 316, XP019125359, ISBN: 978-3-642-03355-1 * section 2, 3 et 5 ***
- **ERIC BRIER ET AL: "Efficient Indifferentiable Hashing into Ordinary Elliptic Curves", 15 août 2010 (2010-08-15), ADVANCES IN CRYPTOLOGY Â CRYPTO 2010, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 237 - 254, XP019147643, ISBN: 978-3-642-14622-0 * sections 2.1, 7 ***
- **JULIEN BRINGER ET AL: "Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters", 22 juin 2010 (2010-06-22), APPLIED CRYPTOGRAPHY AND NETWORK SECURITY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 291 - 308, XP019144595, ISBN: 978-3-642-13707-5 * page 295 ***

EP 2 544 398 B8