



(11) **EP 2 600 561 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 73

(51) Int Cl.:
H04L 9/08 (2006.01) **H04L 9/00 (2006.01)**

(48) Corrigendum issued on:
04.12.2019 Bulletin 2019/49

(45) Date of publication and mention
of the grant of the patent:
23.10.2019 Bulletin 2019/43

(21) Application number: **11191302.6**

(22) Date of filing: **30.11.2011**

(54) **Assessing Cryptographic Entropy**

Beurteilung der kryptografischen Entropie

Évaluation d'entropie cryptographique

(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

(43) Date of publication of application:
05.06.2013 Bulletin 2013/23

(60) Divisional application:
19200234.3

(73) Proprietor: **BlackBerry Limited**
Waterloo, Ontario N2K 0A7 (CA)

(72) Inventor: **Brown, Daniel Richard L**
Mississauga, Ontario L4W 0B5 (CA)

(74) Representative: **Gill Jennings & Every LLP**
The Broadgate Tower
20 Primrose Street
London EC2A 2ES (GB)

(56) References cited:
US-A1- 2010 002 877 US-A1- 2010 106 756
US-A1- 2010 106 757

- **KELSEY J ET AL: "YARROW-160: NOTES ON THE DESIGN AND ANALYSIS OF THE YARROW CRYPTOGRAPHIC PSEUDORANDOM NUMBER GENERATOR", SELECTED AREAS IN CRYPTOGRAPHY. ANNUAL INTERNATIONAL WORKSHOP, XX, XX, 1 August 1999 (1999-08-01), pages 13-33, XP001012490,**
- **Andrew Rukhin ET AL: "A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS", , 15 May 2001 (2001-05-15), pages 1-162, XP55026647, Retrieved from the Internet:
URL:<http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf> [retrieved on 2012-05-09]**
- **Daniel R.L. Brown: "Formally assessing cryptographic entropy", eprint.iacr.org, 9 December 2011 (2011-12-09), XP55026744, Retrieved from the Internet:
URL:[http://eprint.iacr.org/cgi-bin/getfile .pl?entr y=2011/659&version=20111209:210029 &file=659.pdf](http://eprint.iacr.org/cgi-bin/getfile.pl?entr y=2011/659&version=20111209:210029 &file=659.pdf) [retrieved on 2012-05-09]**

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 2 600 561 B8