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

(11) **EP 3 371 928 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

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

(48) Corrigendum issued on:
18.05.2022 Bulletin 2022/20

(45) Date of publication and mention of the grant of the patent:
06.04.2022 Bulletin 2022/14

(21) Application number: **16788725.6**

(22) Date of filing: **02.11.2016**

(51) International Patent Classification (IPC):
H04L 9/06 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
H04L 9/0618; H04L 2209/24

(86) International application number:
PCT/EP2016/076436

(87) International publication number:
WO 2017/076911 (11.05.2017 Gazette 2017/19)

(54) **KEY SEQUENCE GENERATION FOR CRYPTOGRAPHIC OPERATIONS**

SCHLÜSSELSEQUENZGENERIERUNG FÜR KRYPTOGRAPHISCHE OPERATIONEN

GÉNÉRATION DE SÉQUENCE DE CLÉ POUR OPÉRATIONS CRYPTOGRAPHIQUES

(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

(30) Priority: **06.11.2015 GB 201519612**

(43) Date of publication of application:
12.09.2018 Bulletin 2018/37

(73) Proprietor: **Nagravision Sàrl**
1033 Cheseaux-sur-Lausanne (CH)

(72) Inventors:
- **VILLEGAS, Karine**
  1033 Cheseaux-sur-Lausanne (CH)
- **WYSEUR, Brecht**
  1033 Cheseaux-sur-Lausanne (CH)

(74) Representative: **Ipside**
7-9 Allées Haussmann
33300 Bordeaux Cedex (FR)

(56) References cited:
EP-A1- 2 197 144
WO-A1-98/31122
US-A1- 2008 304 664
US-A1- 2009 245 510
US-A1- 2011 138 192
US-B1- 6 185 679

- **JUNOD PASCAL ET AL: "FOX : A New Family of Block Ciphers", 9 August 2004 (2004-08-09), NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 114 - 129, XP047373883, ISSN: 0302-9743 ISBN: 978-3-642-27996-6 cited in the application sections 2.3 and 3.2**
- **RIJMEN VINCENT ET AL: "The cipher SHARK", 21 February 1996 (1996-02-21), NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 99 - 111, XP047294329, ISSN: 0302-9743 ISBN: 978-3-642-23446-0 [retrieved on 2005-06-02] last paragraph of page 104**

EP 3 371 928 B8