



(11) **EP 3 133 766 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 84

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

(48) Corrigendum issued on:
12.08.2020 Bulletin 2020/33

(45) Date of publication and mention
of the grant of the patent:
17.06.2020 Bulletin 2020/25

(21) Application number: **15181508.1**

(22) Date of filing: **19.08.2015**

(54) **COMMUNICATION DEVICE AND METHOD FOR PERFORMING ENCRYPTED COMMUNICATION
IN MULTIPOINT NETWORKS**

KOMMUNIKATIONSVORRICHTUNG UND VERFAHREN ZUR DURCHFÜHRUNG VON
VERSCHLÜSSELTER KOMMUNIKATION IN MEHRPUNKTNETZWERKEN

DISPOSITIF DE COMMUNICATION ET PROCÉDÉ POUR EFFECTUER UNE COMMUNICATION
CRYPTÉE DANS DES RÉSEAUX MULTIPONTS

(84) Designated Contracting States:
**AL AT BE BG CY CZ DE DK EE ES FI FR GB GR
HR HU IS IT LT LU LV MC MK MT NL NO PL PT
RO RS SE SI SK SM TR**

(43) Date of publication of application:
22.02.2017 Bulletin 2017/08

(73) Proprietor: **Rohde & Schwarz SIT GmbH**
12489 Berlin (DE)

(72) Inventors:
• **Graubner, Andreas**
12487 Berlin (DE)
• **Röhrich, Stefan**
10437 Berlin (DE)
• **Heep, Bernhard**
10245 Berlin (DE)

(74) Representative: **Körfer, Thomas**
Mitscherlich PartmbB
Patent- und Rechtsanwälte
Sonnenstrasse 33
80331 München (DE)

(56) References cited:
EP-A2- 0 405 215 EP-A2- 0 669 741
EP-A2- 1 119 132 US-A1- 2009 235 075
US-A1- 2010 042 841

• "Chapter 13: Key Management Techniques ED -
Menezes A J; Van Oorschot P C; Vanstone S A",
HANDBOOK OF APPLIED CRYPTOGRAPHY;
[CRC PRESS SERIES ON DISCRETE
MATHEMATICS AND ITS APPLICATIONS], CRC
PRESS, BOCA RATON, FL, US, PAGE(S) 543 -
590 , 1 October 1996 (1996-10-01), XP001525013,
ISBN: 978-0-8493-8523-0 Retrieved from the
Internet:
URL:<http://www.cacr.math.uwaterloo.ca/hac/>

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 3 133 766 B8

- "Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 , 1 October 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Retrieved from the Internet:
URL:<http://www.cacr.math.uwaterloo.ca/hac/>
- HUIJIE LI ET AL: "GKDA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security", 1 January 2006 (2006-01-01), ADVANCES IN MULTIMEDIA INFORMATION PROCESSING - PCM 2006 LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 310 - 318, XP019047708, ISBN: 978-3-540-48766-1