(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 October 2014 (30.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/174044 A1

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

(21) International Application Number:
PCT/EP2014/058397

(22) International Filing Date:
24 April 2014 (24.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13165184.6 24 April 2013 (24.04.2013) EP

(71) Applicant: **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors: **KARAME, Ghassan**; Heinrich-Fuchs-Strasse 59, 69126 Heidelberg (DE). **SORIENTE, Claudio**; Rossbergstraße 29, CH-8002 Zürich (CH). **CAPKUN, Srdjan**; Bombachstraße 21, CH-8049 Zürich (CH).

(74) Agent: **ULLRICH & NAUMANN**; Schneidmühlstraße 21, 69115 Heidelberg (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: METHOD AND SYSTEM FOR ENCRYPTING DATA

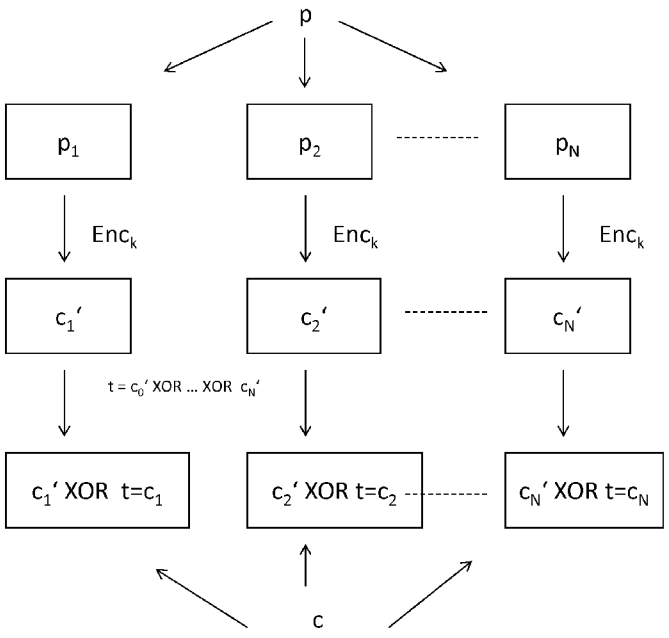

Fig. 2

(57) Abstract: The present invention relates to a method for encrypting data based on all-or-nothing encryption, comprising the steps a) Providing data to be encrypted, preferably in form of a plaintext bitstream, and an encryption key, preferably wherein the encryption key may be secret or publicly known, b) Dividing said data into an odd number of blocks, such that each of said blocks has the same size c) Encrypting said blocks, preferably using symmetric encryption, with said encryption key obtaining an intermediate ciphertext comprising the encrypted blocks, and d) Linear transforming the intermediate ciphertext based on additive contravalence operations to obtain a final ciphertext.

WO 2014/174044 A1