



(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number: PCT/IB2020/001147

(22) **International Filing Date:** 18 December 2020 (18.12.2020)

(25) **Filing Language:** English

(26) **Publication Language:** English

(71) Applicant: **RAVEL TECHNOLOGIES** [FR/FR]; 149, rue Saint-Honoré, 75001 Paris (FR).

(72) **Inventors: KOSKAS, Michel**; 63, rue de la colonie, 75013 Paris (FR). **CHARTIER, Philippe**; 14, rue du haut Sancé, 35000 Rennes (FR). **LEMOU, Mohammed**; 17, rue Henri Cartier Bresson, 35690 Agnès (FR). **MEHATS, Florian**; 20, rue Rabelais, 35000 Rennes (FR).

(74) **Agent:** CAMUS, Olivier et al.; 25 rue de maubeuge, 75009 Paris (FR).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, 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).

(54) Title: HOMOMORPHIC ENCRYPTION METHOD AND ASSOCIATED DEVICES AND SYSTEM

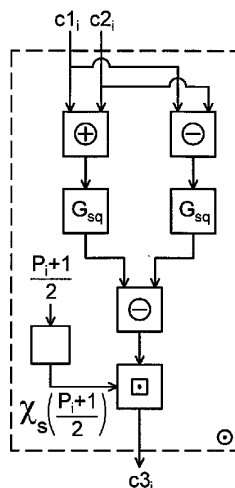


Fig. 1

(57) **Abstract:** The disclosed technology concerns an homomorphic encryption technique that enables to carry on operations on encrypted messages without decrypting them, these encrypted messages being associated to unencrypted messages that belong to a discrete set consisting of p_i distinct elements, with p_i being an odd number, the elements of said discrete set being such that twice the difference between any two of these elements is not an integer number, said discrete set being for instance the discrete torus $T_{p_i} = \{-(p_i-1)/2, -(p_i-1)/2+1, \dots, (p_i-1)/2-1, (p_i-1)/2\}/p_i$. In particular, a specific bootstrapping procedure for such encrypted messages is disclosed. The disclosed technology concerns also an homomorphic encryption technique for carrying on operations on encrypted messages associated to unencrypted messages that belong Z_p , p being equal to the product of r integer numbers p_i , $i=1, r$ that are pairwise coprime. The disclosed technology concerns also associated electronic devices and systems implementing such techniques.

Published:

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