



(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/SG2018/050149

(22) International Filing Date:
28 March 2018 (28.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201702515T 28 March 2017 (28.03.2017) SG

(71) Applicant: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632 (SG).

(72) Inventors: **NGUYEN, Duy Hieu**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **SUN, Sumei**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **WU, Yong Dong**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **LIM, Boon Shyang**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis

Way, #21-01 Connexis South Tower, Singapore 138632 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(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, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, 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, 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: METHOD OF GENERATING A SECRET KEY FOR DATA COMMUNICATION AND KEY GENERATOR THEREOF

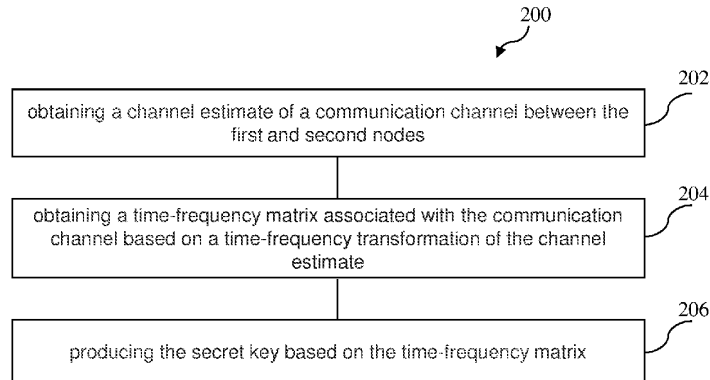


FIG. 2

(57) Abstract: There is provided a method of generating a secret key at a first node for data communication between the first node and a second node. The method includes obtaining a channel estimate of a communication channel between the first and second nodes; obtaining a time-frequency matrix associated with the communication channel based on a time-frequency transformation of the channel estimate; and producing the secret key based on the time-frequency matrix. There is also provided a corresponding key generator for generating a secret key.



Published:

- with international search report (Art. 21(3))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE