

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
06 October 2022 (06.10.2022)



(10) International Publication Number
WO 2022/211731 A1

- (51) International Patent Classification:
H04L 9/08 (2006.01)
- (21) International Application Number:
PCT/SG2022/050172
- (22) International Filing Date:
29 March 2022 (29.03.2022)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10202103245X 30 March 2021 (30.03.2021) SG
- (71) Applicant: **SPEQTRAL PTE. LTD.** [SG/SG]; 73 Science Park Drive, #03-06 Cintech-1, Singapore 118254 (SG).
- (72) Inventors: **BEDINGTON, Robert**; c/o SpeQtral Pte Ltd, #03-06 Cintech 1, 73 Science Park Drive, Singapore 118254
- (SG). **VERGOOSSEN, Tom**; c/o SpeQtral Pte Ltd, #03-06 Cintech 1, 73 Science Park Drive, Singapore 118254 (SG).
- (74) Agent: **LINDSAY, Jonas Daniel**; Marks & Clerk Singapore LLP, Tanjong Pagar Post Office, P.O. Box 636, Singapore 910816 (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, IT, JM, 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,

(54) Title: SECURE SYMMETRIC KEY DISTRIBUTION

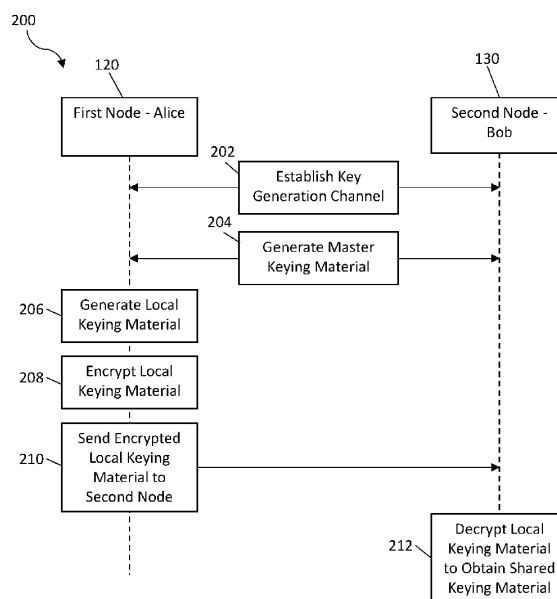


FIG.2

(57) Abstract: Methods, nodes and systems for secure symmetric key distribution are described. A method of creating symmetric keying material shared between a first node and a second node is provided. The method comprises: establishing a key-generation channel between the first node and the second node; generating shared symmetric master keying material using physical layer security methods on the key-generation channel; generating random numbers as local keying material on the first node; encrypting the local keying material using some or all of the shared symmetric master keying material to generate encrypted local keying material on the first node; sending the encrypted local keying material from the first node to the second node over a communication channel; and decrypting the encrypted local keying material on the second node using the corresponding shared symmetric master keying material to create symmetric keying material.

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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